

Systems Insight Manager 7.2 User Guide

HP Part Number: 601823-007
Published: March 2013
Edition: Edition 2



Legal Notices

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Acknowledgments

Microsoft, Windows, Windows Server, Windows Vista, Windows NT, and Windows XP are U.S. registered trademarks of Microsoft Corporation. Linux is a U.S. registered trademark of Linus Torvalds.

Warranty

HP will replace defective delivery media for a period of 90 days from the date of purchase. This warranty applies to all Insight Management products.

Contents

I Introduction.....	13
1 About this document.....	14
User Guide.....	14
HP SIM User Guide layout.....	14
2 Product overview.....	15
HP SIM features.....	15
Basic concepts.....	16
Discovery and identification.....	16
Inventory.....	16
Status info.....	16
Reports.....	16
Automatic event handling.....	17
Tools and tasks.....	17
Collections.....	17
Users and Authorizations.....	17
Nested user groups.....	17
Signing in and using the graphical user interface.....	18
User/System credentials.....	18
Security Alerts in Internet Explorer and Firefox.....	18
Automatically signing in.....	18
Configuring the CMS.....	19
Configuring the browser.....	19
Behavior.....	20
Guided tour of the HP SIM user interface.....	20
Customizing views.....	21
II Setting up HP SIM.....	22
3 Setting up managed systems.....	23
Configure or Repair Agents.....	23
Setting up Windows servers to be managed by HP SIM.....	23
Setting up HP-UX servers to be managed by HP SIM.....	30
Manually setting up an HP-UX managed system.....	31
Configuring SNMP to send traps to the CMS.....	31
Configuring SSH access.....	31
Subscribing to WBEM indications/events.....	31
Setting up Linux servers to be managed by HP SIM.....	32
Configuring agents remotely using Configure or Repair Agents.....	32
Manually setting up Linux managed systems.....	32
Installing and configuring SSH.....	33
Configuring a Linux system to send SNMP traps.....	33
4 Credentials.....	35
Example XML file to add more than 10 WBEM username and password pairs.....	35
5 WMI Mapper Proxy	37
6 Discovery.....	38
Recommended discovery tasks.....	38
Options on the Discovery page.....	39
Discovery credentials.....	40
Configuring Configure or Repair Agents through a discovery task.....	40
Viewing discovery task results.....	40

Discovery filters.....	40
Discovery of Gen8 servers.....	41
7 Manage Communications.....	42
Configuring the managed system software using the Configure or Repair Agents feature from the CMS.....	42
Sending test traps and indications.....	43
8 Automatic event handling.....	44
Example automatic event handling tasks.....	45
9 Users and Authorizations.....	46
Users.....	46
User groups.....	46
Toolboxes.....	46
10 Managed environment.....	47
III HP SIM basic features.....	48
11 Basic and advanced searches.....	49
Basic search.....	49
Advanced search.....	49
Hierarchical displays.....	49
Save as.....	49
View.....	50
Searching for tools.....	50
12 Monitoring systems.....	51
Viewing system collections.....	51
Pages displaying system status.....	51
Viewing health status from the table or icon view.....	52
Viewing health status in the tree view.....	52
System status types.....	52
Software status types.....	53
WBEM operational status types.....	54
Monitoring clusters.....	54
System properties.....	55
Example of setting system properties.....	56
Setting customer company and contact information individually.....	56
Example of setting system properties for multiple systems.....	56
13 Event management.....	57
Event management configuration.....	57
Example - Creating a paging task based on e-mail notification.....	58
Examples of e-mail pages.....	59
Example of a standard e-mail page.....	59
Example of a Pager/SMS page.....	60
Example of an HTML page.....	60
Example - Creating a task to send an e-mail when a system reaches a critical state.....	61
Example - Creating a task to delete all cleared events.....	62
14 Reporting in HP SIM.....	64
Standard reports.....	64
New Reports.....	64
Managing reports.....	64
Snapshot Comparison.....	65
Enhanced Reports.....	65
Predefined reports.....	66
Run Enhanced reports.....	66

New Enhanced reports.....	67
Editing Enhanced reports.....	67
E-mailing reports.....	67
Deleting reports.....	67
15 HP SIM tools.....	69
Target selection.....	69
Scheduling tools.....	69
Managing with tasks.....	69
Viewing results.....	70
Example - Device ping.....	70
IV HP SIM advanced features.....	71
16 Collections in HP SIM.....	72
Collections in HP SIM.....	72
Types of collections.....	73
Creating a System Collection.....	74
Other customization features.....	74
17 HP SIM custom tools.....	79
General concepts.....	79
Tool types.....	79
Environment variables for custom tools.....	80
Launching applications using custom tools.....	82
Custom tool menu placement.....	82
Custom tool URL format.....	82
Creating custom tools through the GUI.....	83
New.....	83
Edit.....	83
View tool definition.....	84
Run Now/Schedule.....	84
Delete.....	84
Creating custom tools through the HP SIM CLI.....	84
Creating a custom SSA tool.....	84
Example Web launch tool.....	87
Example MSA tool.....	87
Example Enabling Remote Desktop tool.....	88
Adding a TDEF to HP SIM.....	89
Removing a TDEF from HP SIM.....	89
Modifying a TDEF.....	90
18 Federated Search.....	91
Federated CMS Configuration.....	91
19 CMS Reconfigure Tool.....	93
Operational Commands, Options and Parameters.....	93
Reconfiguring the CMS password.....	93
Dependencies.....	94
Warnings.....	94
Changing the CMS password.....	94
Reconfiguring the CMS host and IP attributes.....	95
Dependencies.....	96
Warning.....	96
Reconfiguring the CMS host name and primary IP address.....	96
Reconfiguring the CMS database credentials.....	96
Dependencies.....	97
Warning.....	97

Changing the HP SIM and HP Insight Control database credentials.....	97
Changing the database authorizations for Matrix OE and HP Operations Orchestration....	97
Reconfiguring the CMS to use a different database.....	98
Dependencies.....	98
Warning.....	98
Changing the database associated with the CMS.....	98
20 Understanding HP SIM security.....	100
Securing communication.....	100
Secure Sockets Layer (SSL).....	100
How to configure ciphers.....	100
Secure Shell (SSH).....	100
Hyper Text Transfer Protocol Secure (HTTPS).....	100
Secure Task Execution (STE) and Single Sign-On (SSO).....	100
Distributed Task Facility (DTF).....	101
WBEM.....	101
LDAP.....	101
RMI.....	101
Credentials management.....	101
SSL certificates.....	101
HP SIM main certificate.....	101
HP SIM SSO certificate.....	102
WBEM certificate.....	102
Upgrading to HP SIM 7.2.....	102
Certificate expiration and Certificate Revocation Check (CRL Check).....	102
Source of client and server certificates.....	102
Enabling or disabling certificate revocation check.....	103
Offline and online mode of certificate revocation check.....	103
Offline mode.....	103
Online mode.....	103
CRL distribution points.....	103
Warning or error.....	104
Conditions for warning.....	104
Customizable properties.....	104
Certificate sharing.....	104
SSH keys.....	104
Passwords.....	105
Insight Control for VMware vCenter Server server authorizations.....	105
Browser.....	106
SSL.....	106
Cookies.....	106
Passwords.....	106
Password warnings.....	106
Browser session.....	107
Internet Explorer zones.....	107
System link format.....	107
Operating-system dependencies.....	107
User accounts and authentication.....	107
File system.....	108
Background processes.....	108
Windows Cygwin.....	108
HP-UX and Linux.....	108
HP SIM database.....	108
Configuring the SQL Server to enable SSL connection on database in HP SIM.....	108
Installing a certificate on a server with Microsoft Management Consold (MMC).....	109

Configuring SSL for SQL Server.....	109
Configuration of client to enable trust.....	110
How to test your client connection.....	110
HP SIM database property settings to enable SSL for SQL Server.....	110
SQL Server and MSDE.....	111
Remote SQL Server.....	111
PostgreSQL.....	111
Oracle.....	111
Command-line interface.....	111
How to: configuration checklist.....	112
General.....	112
Configuring the CMS.....	112
Strong security.....	112
Configuring managed systems.....	112
How to: lockdown versus ease of use on Windows systems.....	113
Moderate.....	113
Strong.....	114
21 Privilege elevation.....	116
Two-factor authentication.....	116
Enabling and disabling two-factor authentication.....	116
Enable secure communication.....	117
Directory structure users.....	117
Users Distinguished Name.....	117
Subject Alternative Name.....	117
Authentication phase.....	117
Authorization phase.....	117
Certificate revocation check.....	117
Pre-requisites to enable two-factor authentication technique.....	117
Smart cards and Cryptographic Service Provider (CSP).....	118
Security measures to follow.....	118
22 HP SIM quiesce.....	119
23 Contract and warranty.....	120
Viewing contract and warranty information.....	120
Collecting contract and warranty data.....	121
Viewing contract and warranty status.....	121
Overview.....	121
System Information.....	121
Contract.....	121
Warranty.....	122
Monitoring contract and warranty status.....	124
24 License Manager.....	125
CLI mxlmkeyconfig.....	126
License types.....	126
Licensed System(s).....	128
Add Licenses.....	128
Collect Remote License Info.....	128
License Collection Results table.....	128
Assigning and Unassigning licenses.....	130
Apply Licenses.....	130
Add License page.....	131
Key details page.....	131
Assigning or Applying Licenses page.....	132
License unlicensed systems (optional) page.....	133

25 Storage integration using SMI-S.....	134
About storage systems.....	134
Storage integration using SNMP.....	134
Storage events.....	135
Storage inventory details.....	135
Introduction to SMI-S for HP SIM.....	136
About SMI-S.....	136
Key components.....	136
CIM.....	136
WBEM.....	137
SLP.....	137
Profiles.....	137
SMI-S implementation.....	137
About storage security using SNMP.....	137
Discovery and identification.....	137
Prerequisites for managing storage systems.....	138
Using storage solutions.....	138
Event collection and launch.....	138
For Command View SDM.....	138
Configuring the SNMP trap destination on Windows 2000.....	139
Configuring the SNMP trap destination on HP-UX.....	139
Loading the HSV MIB on the CMS for EVA.....	139
Receiving WBEM protocol events from XP arrays.....	139
Discovery.....	140
Configuring HP SIM with storage systems.....	140
Subscribe to WBEM indication events.....	140
Viewing storage system collections.....	141
Viewing individual storage systems.....	141
Viewing storage system reports.....	141
Existing storage system reports.....	141
Viewing storage array capacity.....	142
Viewing storage capacity for all arrays.....	142
Viewing storage capacity for a single array.....	142
26 Managing MSCS clusters.....	143
MSCS status.....	143
Cluster fields.....	144
Node fields.....	144
Network fields.....	144
Resource fields.....	145
Cluster Monitor resource thresholds.....	145
Disk capacity thresholds.....	145
CPU utilization thresholds.....	145
Cluster resources supported by HP SIM.....	146
Cluster Monitor states.....	146
Cluster Monitor polling rate.....	146
CPU polling rate.....	146
Disk polling rate.....	147
MSCS status polling rate.....	147
System status polling rate.....	147
27 HP SIM Audit log.....	148
Configuring the HP SIM audit log.....	148
Configuring the tool definition files.....	148
Configuring the log.properties file	148
Viewing the audit log.....	148

Example audit log.....	148
Log content.....	149
28 HP Version Control and HP SIM.....	150
About the Version Control Agent.....	150
Additional resources.....	150
About the Version Control Repository Manager.....	151
About integration.....	151
About software repositories.....	152
About multiple system management.....	152
29 Compiling and customizing MIBs.....	154
MIB management tools.....	154
mcompile.....	154
mxmib.....	156
mxmib MIB keyword customization.....	157
SNMP Trap Settings page.....	160
30 Proxy authenticator.....	162
Requirements.....	162
Proxy authenticator additional information.....	162
Settings to be made in HP SIM.....	163
Configuring trust check in HP SIM for Proxy authenticator server.....	166
How to use Proxy authenticator.....	166
A Important Notes.....	167
System and object names must be unique.....	167
Setting the Primary DNS Suffix for the CMS.....	167
Distributed Systems Administration Utilities menu options not available.....	167
Virtual machine guest memory reservation size.....	167
Insight Remote Support Advanced compatibility.....	167
Database firewall settings.....	168
Annotating the portal UI.....	168
Security bulletins.....	168
Validating RPM signatures.....	169
Checking which public keys are installed.....	169
Validate the signature on an RPM.....	169
How to check RPM signatures within the sysmgmt.bin.....	169
Central Management Server.....	170
Complex systems displaying inconsistency with the number of nPars within the complex.....	170
Configure or Repair Agents.....	171
Data collection reports.....	171
B Troubleshooting.....	172
Adobe.....	172
Agentless Management Service.....	172
Authentication.....	172
Blade insertion.....	172
Browser.....	173
Central Management Server.....	174
Complex.....	175
Configure or Repair Agents.....	175
Container View.....	176
Credentials.....	177
Data Collection.....	177
Database.....	179
Discovery.....	179

iLO.....	182
Linux servers.....	182
Enclosure table view page.....	182
Event.....	182
Health status.....	183
Host name.....	183
HP Insight Control power management.....	183
Insight Control virtual machine management.....	185
HP Smart Update Manager.....	185
HP Service Pack for ProLiant.....	187
HP Systems Insight Manager.....	187
Identification.....	187
Installation.....	189
License Manager.....	190
Locale.....	190
Managed Environment.....	190
HP MIBs.....	191
Onboard Administrator.....	191
OpenSSH.....	191
Performance.....	191
Ping.....	192
Ports used by HP SIM.....	192
Privilege elevation.....	193
Property pages.....	193
Reporting.....	193
Security.....	193
Sign-in.....	194
SNMP settings.....	194
SNMP traps.....	194
SSH communication.....	194
Software/Firmware.....	194
System Page.....	194
System status.....	194
Target selection wizard.....	194
Tasks.....	195
Tools.....	195
Ubuntu.....	195
Upgrade.....	196
UUID.....	196
Virtual Connect Enterprise Manager.....	196
Virtual identifiers.....	196
Virtual machines.....	197
VMware.....	198
WBEM.....	198
WBEM indications.....	198
WMI Mapper.....	198
C HP SIM Dynamic Ports.....	200
Windows 2003.....	200
Microsoft Windows Vista, Microsoft Windows 2008 and Above.....	201
D Protocols used by HP SIM.....	202
SNMP.....	202
Windows.....	202
HP-UX and Linux.....	203
HTTP.....	204

WBEM.....	204
Remote Method Invocation (RMI).....	205
Remote Wake-Up.....	205
Internet Control Message Protocol (ICMP).....	205
Lightweight Directory Access Protocol (LDAP).....	205
Simple Object Access Protocol (SOAP).....	205
Protocol functionality.....	205
Configuring protocol settings in HP SIM.....	207
E Data Collection.....	208
Append new data set (for historical trend analysis).....	208
Overwrite existing data set (for detailed analysis).....	208
Initial data collection.....	208
Bi-weekly data collection.....	209
F Default system tasks.....	210
Biweekly Data Collection.....	211
System Identification.....	211
Old Noisy Events.....	212
Events Older Than 90 Days.....	212
Status Polling for Non Servers.....	212
Status Polling for Servers.....	212
Status Polling for Systems No Longer Disabled.....	212
Hardware Status Polling for Superdome 2 Onboard Administrator.....	212
Data Collection.....	212
Hardware Status Polling.....	212
Version Status Polling.....	212
Version Status Polling for Systems no Longer Disabled.....	213
Check Event Configuration.....	213
Status polling.....	213
G Host file extensions.....	214
Default values.....	216
H System Type Manager rules.....	218
Adding new SNMP rules.....	218
I Custom tool definition files.....	219
Tool type-specific requirements.....	219
SSA-specific attributes.....	219
MSA-specific attributes.....	219
WLA-specific attributes.....	220
mxtool command parameters.....	221
Parameterized strings.....	221
Common tool attributes.....	223
Tool Filtering attributes.....	225
Environment Variables.....	225
Tool parameter guidelines.....	227
J Out-of-the-box MIB support in HP SIM.....	229
K Support and other resources.....	234
Information to collect before contacting HP.....	234
How to contact HP.....	234
Security bulletin and alert policy for non-HP owned software components.....	234
Subscription service.....	234
Registering for software technical support and update service.....	234
How to use your software technical support and update service.....	235
HP authorized resellers.....	235

Related documents.....	235
Documentation and support.....	235
HP SIM documentation.....	236
Typographic conventions.....	236
Documentation feedback.....	236
Glossary.....	237
Index.....	247

Part I Introduction

1 About this document

User Guide

HP Systems Insight Manager provides this user guide to help you understand management features.

HP SIM User Guide layout

- **Introduction**
Describes the features, basic concepts, and using the [graphical user interface](#) (GUI) in HP SIM.
- **Setting up HP SIM**
Describes how to set up HP SIM by explaining requirements for systems to be managed by HP SIM, credentials, discovery, automatic event handling, and users and [authorizations](#).
- **HP SIM basic features**
Describes HP SIM basic features, including monitoring systems, clusters, and events, performing basic and advanced searches, editing system properties, and basic reporting.
- **HP SIM advanced features**
Describes HP SIM advanced features, including managing with [collections](#), advanced reporting, and creating custom tools.

For information on HP SIM support and how to access related documentation, see [“Support and other resources”](#) (page 234).

2 Product overview

HP SIM features

- **Automatic discovery**

Automatically discovers and identifies systems attached to the network. Use [discovery filters](#) to prevent discovery of unwanted system types.
- **Health monitoring**

Colored status icons enable you to see at a glance the operational health of your systems, and quickly drill down to find the failing component if any are not ok.
- **Fault management and event handling**

HP SIM provides proactive notification of actual or impending component failure alerts. Automatic Event Handling enables you to configure actions to notify appropriate users of failures through e-mail or pager, and enables automatic execution of scripts or [event forwarding](#) to enterprise platforms such as [HP Operations Orchestration](#) or [HP Network Node Manager](#).

NOTE: Pager support is only for Windows-based [Central Management Server \(CMS\)](#).

- **HP SIM Quiesce**

Criticality button enables the task to be completed without cancelling.

Commands:

```
mxquiesce -u Administrator -p [password]
mxunquiesce -u Administrator -p [password]
```
- **Inventory**

Performs comprehensive system data collection and enables users to quickly produce detailed inventory reports for [managed systems](#). Save reports in multiple formats for easy incorporation into popular reporting packages.
- **Consistent multisystem management**

HP SIM initiates a task on multiple systems or nodes from a single command on the CMS. This functionality eliminates the need for tedious, one-at-a-time operations performed on each system.
- **Role-based security**

Allows effective delegation of management responsibilities by giving systems administrators granular control over which management operations users can perform on selected systems.
- **Two user interfaces**

HP SIM provides the option of a browser-based GUI or a [command line interface \(CLI\)](#) that enables you to incorporate HP SIM into your existing management processes.
- **Customized tools**

Simple Extensible Markup Language (XML) documents that enable you to integrate off-the-shelf or custom command line and web-based applications or scripts into the HP SIM user interface.

Basic concepts

Discovery and identification

HP SIM can automatically discover and identify systems attached to the network using information from management protocols such as [Simple Network Management Protocol](#) (SNMP, SNMPv3), [Windows Management Instrumentation](#) (WMI), WBEM, [Secure Shell](#) (SSH), [Secure Sockets Layer](#) (SSL), HTTP/HTTPS, and WS-MAN. Create discovery tasks to limit discovery to specific network segments or IP address ranges, or to control the frequency that each task runs. Use discovery filters to prevent discovery of unwanted system types.

NOTE: HP SIM uses several management protocols to communicate to managed systems. The protocols used, include WBEM/WMI, SNMP, SNMPv3, HTTP/HTTPS, SSH and WS-MAN. All of these protocols can be configured to access data from non-root/non-administrator users. For Linux systems, one of the protocols used during discovery, is SSH. During discovery, HP SIM executes the command, `/usr/sbin/dmidecode`, on the remote Linux system to fetch certain information. Since this command requires super user privileges, HP SIM needs the root credentials. Therefore, to discover a Linux system using SSH protocol, be sure root credentials are entered as part discovery, system or global credentials

Inventory

[Data collection](#) gathers data that can be used for reporting and to populate various fields in the user interface. HP SIM collects various information such as system type and sub-type, supported protocols, and available memory. You can choose to maintain only the most recent data, enabling you to run reports or compare different systems using Snapshot Comparison. Or, you can store all data collected over time, which enables use of Snapshot Comparison to view trends on a single system.

Status info

The following status icons are used in the status list columns to show status on different aspects of the managed systems. For example, the **MP** column displays the status icon of the management processor if the system has a management processor board installed.

Table 1 Status types

Status icon	Status type
	Critical
	Major
	Minor
	Warning
	Normal
	Disabled
	Unknown
	Informational

Reports

HP SIM performs comprehensive system data collection and enables you to quickly produce detailed inventory reports for managed systems. Reports can be generated in Hyper Text Markup Language (HTML), XML, or Comma Separated Value (CSV) format. Enhanced reports can be automatically

generated and e-mailed on a scheduled basis. The type of data collected depends on the management software (SNMP agents or WBEM/WMI providers) that is installed.

Automatic event handling

Automatic event handling enables you to define an action that HP SIM performs when an event is received. These actions can include running a program or script, forwarding the event to another management system, clearing the event, or notifying a user through e-mail or pager.

Tools and tasks

Tools are actions you perform on the managed systems from within HP SIM's GUI or CLI. Many tools ship with HP SIM, but you can also add your own custom tools. Tasks are instances of running tools. To create a task, select **target systems** (systems or events that the task will work on) and then select the tool from the HP SIM menu. Tasks can be run immediately or scheduled, and you can view task results by selecting **Tasks & Logs**→**View Task Results**.

Tools can be run from the HP SIM menus and can be added to a Quick Launch list that is available from many pages within HP SIM.

Collections

Collections are groups of systems and events that can be used for viewing information, or as a way to specify the targets for a tool. They can be created through the **Customize** link in the **System and Event Collections** panel either by selecting specific systems to be included, or by specifying attributes to be matched. Once created, they are displayed in the **System and Event Collections** panel for quick access. Shared collections can be seen by everyone logging into HP SIM. Private collections can only be seen by the user who created them.

You can bind event collections and system collections together and use them either separately or together. For example, after you define a collection of **Security Events**, you can easily look at those events on any system collection, such as **Security Events on All Servers** or **Security Events on My FinancialServers**.

Conversely, you can choose a system collection, and view any set of events on those systems. For example, you can easily select **My FinancialServers** and look at **All Events**, **Sign-in Events**, **Security Events**, or any other event collection as it applies to that collection of systems.

Users and Authorizations

HP SIM enables effective delegation of management responsibilities by giving system administrators granular control over which users can perform specific management operations on specific systems.

Nested user groups

A nested user group is a concept on Windows Active Directory. A user/user group might belong to one or many user groups. Therefore, it makes a hierarchical relationship between users and user groups.

For Windows to support nested group security; CMS, user and user groups must exist in Active Directory. Members of user groups (user and user group) inherit the behavior (authentication and authorization privilege) from its parent groups. So, if a user is a member of two different user groups with different privileges and one group is a member of another user group, then the user will inherit rights as a result of the union of all the three user groups.

If a user is a member of more than one user group, then the IP login restrictions of all the user groups are combined and applied to the user. To override IP login restrictions of all user groups with the user's current group IP login restrictions, select **Override IP Login Inclusion/Exclusion Range** from the user's authorizations page.

Signing in and using the graphical user interface

HP SIM provides a browser-based GUI. Supported browsers include:

- For Windows:
 - Microsoft Internet Explorer 8 or later
 - Firefox 3.x, 6.x, 9.x, 10.x, and Firefox ESR
- For HP-UX:
Firefox 3.5.09.00 or later
To download, go to <http://www.hp.com/go/firefox>.
- For Linux:
Firefox 9 or later

NOTE: Browser settings:

- For all Windows Internet Explorer browsers, you must have the SSL 3.0 or Transport Layer Security (TLS) 1.0 browser security options enabled for HP SIM to work properly, which allows only stronger ciphers for the SSL connection.
 - To use automatic sign-in with Firefox, you must configure Firefox with a list of sites with automatic sign-in. For more information, see *Initial setup* section of the HP SIM online help.
-

User/System credentials

- Due to security reasons and to avoid security threats, HP SIM does not allow empty password or passwords containing empty space(s) only
- A user/system password can contain empty spaces but it should not start or end with an empty space

Security Alerts in Internet Explorer and Firefox

Because the HP SIM web server uses a self-signed SSL certificate (unless otherwise configured), you will encounter a browser warning when browsing to the CMS. Firefox warns of an *Untrusted Connection*. Internet Explorer warns of a *Certificate Error*. Both browsers let you continue, but you can take measures to avoid repeatedly encountering those warnings. This applies to HP SIM, HP SMH, Integrated Lights-Out (iLO), Onboard Administrator, and all web servers you browse to.

Each time you receive an *Untrusted Connection* warning in Firefox, you must add a *permanent* security exception to avoid seeing the warning again for that host. Note that if you browse to a single system using its short host name, fully qualified Domain Name Service (FQDN), and IP address (for example, three different ways), you must add three security exceptions.

With Internet Explorer, you must install the SSL certificate into the **Trusted Root Certification Authorities** certificate store, but the browser will continue to warn you (by default) when details in the certificate do not match (for example, browsing by short host name when the full host name is in the certificate). To avoid certificate errors when names do not match, the following setting must be turned off: **Internet Explorer**→**Advanced**→**Security**→**Warn about certificate address mismatch**.

If you do not install the SSL certificate in Internet Explorer 8, these warnings appear for each pop-up window that appears in HP SIM.

Automatically signing in

You can sign in to HP SIM using the same account with which you are logged in on your desktop, bypassing the HP SIM sign-in page. If user groups are configured for HP SIM, membership in these groups is accepted and treated the same as if you manually signed in.

Configuring the CMS

- HP SIM must be running on a Windows CMS that is a member of a Windows domain. The browsing system must be a member of the same domain.
- The HP SIM service account must be a domain account; local accounts can not be used.
- The CMS must be registered with an SPN in the domain, which requires a domain administrator to configure. From any system that is a member of the domain, the domain administrator can run the `setspn.exe` utility from the Windows Support Tools. For example:

```
setspn -a HTTP/<cms_fqdn> <sim_service_account>
```

Where HTTP is in all capital letters, `<cms_fqdn>` is the FQDN of the CMS, and `<sim_service_account>` is the domain account under which HP SIM service runs.

- ① **IMPORTANT:** Automatic sign-in fails if the SPN registered more than once. If you change the name of the HP SIM service account, you must first delete the SPN associated with the old service account name, and then register the new service account name:

```
setspn -d HTTP/<cms_fqdn> <old_sim_service_account>
```

```
setspn -a HTTP/<cms_fqdn> <new_sim_service_account>
```

NOTE: Local accounts cannot be used for HP SIM service account if automatic sign-in is desired.

- The automatic sign-in feature must be enabled in HP SIM in the `globalsettings.props` file. You can use the `mxglobalsettings` command, or directly modify the file. Set the value for the `AutomaticSignIn` property to 1. Restarting HP SIM is not necessary.

Configuring the browser

- Supported in Internet Explorer 8, Internet Explorer 9, Internet Explorer 10 and Firefox. Internet Explorer 7 is not supported.
- The browsing system must be remote; browsing locally from the CMS does not perform automatic sign-in.
- The browsing system and the CMS must be members of the same Windows domain.
- You must be logged in to the browsing system with a domain account that is configured as a user account in HP SIM, or is a member of a user group configured in HP SIM.
- There must be no proxy servers between the browser and the CMS. Use the proxy bypass list in the browser, or use no proxy at all.
- The browser must be configured to support automatic sign-in.
- The remote browsing machine must use Adobe 10. Adobe 11 is not supported.

Procedure 1 Configuring the browser in Internet Explorer

1. In Internet Explorer, enable **Integrated Windows Authentication** under **Tools**→**Internet Options**→**Advanced** tab.
2. The CMS must be in the **Local Intranet** or **Trusted Sites** zone, which can be configured under the **Tools**→**Internet Options**→**Security** tab.
3. (Optional) If the CMS is in the Internet Explorer Local Intranet zone, select **Automatic Logon only in Intranet zone**.
4. (Optional) If the CMS is in the Internet Explorer Trusted Sites zone, select **Automatic logon with current user name and password**.

Configuring the browser in Firefox:

Firefox must be configured with a list of sites (for example, the CMS) where automatic sign-in can be performed, and should be restricted to local intranet sites. This list can be configured by entering

about:config in the Firefox address bar. From the list of **Preference Names**, select **network.negotiate-auth.trusted-uris** and either double-click or right-click, and select **Modify**. Here, you can specify a comma-separated list of URLs or domains, enter the list of URLs used to access HP SIM. For example: `https://cms_fqdn`, where `cms_fqdn` is the FQDN of the CMS.

Behavior

When automatic sign-in occurs, an intermediate sign-in page appears. If you click **Cancel** from this page, the manual sign-in page appears. You might want to cancel automatic sign-in if any unexpected network or domain errors occur. If any browser configuration errors are detected, automatic sign-in is cancelled and the manual sign-in page appears along with the configuration error.

Failures encountered during automatic sign-in are logged as normal sign-in failures in both the audit log and the event log. If automatic sign-in is not attempted, no failure is detected or logged by HP SIM.

If automatic sign-in is configured, you can manually sign in to HP SIM.

- **If automatic sign-in fails, the manual sign-in page appears**

This might occur if you are logged in to the operating system using an account that is not an HP SIM account.

- **If automatic sign-in is not attempted**

This might occur if the browser is not properly configured for automatic sign-in, or the feature is disabled in HP SIM.

- **If you click Sign Out from HP SIM**

This enables you to specify another user account to use if you are signed in to the operating system with a different account.

Guided tour of the HP SIM user interface



The GUI includes the following six regions:

1. Banner area

The [banner](#) provides a link to the **Home** page, a link to **Sign Out** of HP SIM, and displays the user that is currently signed in. Click the minimize icon in the top right corner to minimize the banner. To maximize the banner, click the maximize icon.

2. System Status panel

This panel provides uncleared event status, [system health status](#) information, and an alarm to notify you about certain events or statuses. You can customize the **System Status** panel for your environment. If you do not need to view this panel at all times, you can collapse it by clicking the minus sign (▢) in the top right corner of the panel. To expand the panel, click the plus sign (▣). If the **System Status** panel is collapsed and an alarm is received, the panel expands to show the alarm. You can enlarge the panel by clicking the **Open in new window** icon (⌵) to display a separate large window that you can resize and view from across a room without sitting at the HP SIM terminal.

3. Search panel

The search feature enables you to search for matches by system name and common system attributes. You can also perform an advanced search for matches based on selected criteria. To speed the search process, as you enter system information in the search box, a dropdown list appears listing systems that begin with the text you are entering. You can select from the dropdown list or continue to enter the information. If you do not need to view this panel at all times, you can collapse it by clicking the minus sign (▢) in the top right corner of the panel. To expand the panel, click the plus sign (▣).

4. System and Event Collections panel

System and event collections enable you to view all known systems and events in a specific management environment. A collection can be private, visible only to its creator, or shared, visible to all users. All default collections are shared. You can add additional collections by clicking the **Customize** link. Collections can optionally be configured to show [health status](#) icons in this area.

5. HP SIM menus

The HP SIM menus provide access to tools, logs, software options, and online help. The **Options** menu is primarily for users who administer the HP SIM software. If you lack authorization to use these tools, you might not be able to view certain menus.

6. HP SIM workspace

The workspace displays the results of your latest request. It can contain a collection, [tool](#), or report. Some tools launch a separate browser window or X Window terminal instead of displaying in the [workspace](#). This area contains the **Home** page when you sign in to HP SIM. By default, the introductory page is the **Home** page. The introductory page provides information and tips about HP SIM and links to frequently used features. You can customize HP SIM to display a different page as the **Home** page.

NOTE: To maximize the workspace, click the **Maximize** link next to the Help icon (⌵). To restore the workspace to its original size, click **Restore Size**.

Customizing views

A **Customize** link is available in the upper right of many pages in HP SIM. Use this link to customize the way the page is presented.

Part II Setting up HP SIM

3 Setting up managed systems

Setting up managed systems involves installing the required Management Agents software and configuring the supported protocols to communicate with the HP SIM software.

Configure or Repair Agents

Managed systems must be able to communicate status to the HP Systems Insight Manager CMS in order to launch commands to the managed systems. To configure the managed systems to communicate with the CMS, you must configure common configurations and trust relationships. The Configure or Repair Agents feature enables you to configure or repair agents in Windows, Linux, and HP-UX.

The Configure or Repair Agents tool enables you to repair [Simple Network Management Protocol](#) settings and trust relationships that exist between HP Systems Insight Manager and target systems if you have 7.2 agents or later installed. If you have 7.1 agents or earlier installed, you can update Web Agent passwords on target systems.

This tool adds the security and trap community strings and trust settings to the target systems, but it does not replace existing settings. To replace existing settings on target systems, use the Replicate Agent Settings feature in HP SIM.

You can use Configure or Repair Agents tool to send test SNMP traps from Windows systems with Insight Management Advisors and send test [Web-Based Enterprise Management](#) indications from Windows and HP-UX systems with HP WBEM provider installed.

You can also configure WBEM certificates for HP-UX systems and WBEM/WMI users for Windows systems with HP Insight Management WBEM Providers for Windows Server 2003 or Windows Server 2008.

The Configure or Repair Agents feature on a Windows CMS also enables you to install various agents and providers on a ProLiant or Itanium-based system with Windows operating system. You can configure certificate based access to HP Version Control Repository Manager from HP Version Control Agent A few features that can be installed include:

- Agentless Management Service (AMS)
- HP Insight Management WBEM Providers for Windows Server 2003 or Windows Server 2008
- OpenSSH
- HP Version Control Agent for Windows
- HP Insight Management Agents for Windows

For detailed information on running Configure or Repair Agents, see the HP SIM online help.

Setting up Windows servers to be managed by HP SIM

To be fully managed by HP SIM, HP ProLiant servers running Windows should have the Insight Management Agents or HP WBEM Providers installed. These agents are part of the ProLiant Support Pack. See the HP SIM online help for instructions on how to do this through the HP SIM UI. You can also configure these agents to be installed as part of your normal operating system deployment procedures. For third party servers, enable WMI and/or SNMP in the operating system. HP SIM attempts to retrieve information that is instrumented in an industry-standard way. After setting up the management agents on the managed systems, the remaining configuration can be done from the HP SIM user interface. Continue to Chapter 4 [“Credentials”](#) (page 35) for further information.

Procedure 2 Configuring or repairing the agents for Windows

1. Select **Configure**→**Configure or Repair Agents**.

2. Select **Install Agentless Management Service (AMS) on HP ProLiant Gen8 servers running Windows, Linux, or ESX** to send all host operating system-specific data to the iLO4 firmware.
3. Select **Install Linux PSP or ESX Agents** to install Linux PSP and ESX Agents which are a collection of SNMP agents used by HP SIM to gather information from managed systems and send traps to HP SIM.
4. Select **Install WBEM / WMI Provider (HP Insight Management WBEM Provider) for Windows** to install WBEM or [WMI](#) providers on Windows managed systems.
5. Select **Install SNMP Agent (Insight Management Agent) for Windows** to install the [SNMP](#) agent on Windows managed systems. This Insight Management Agent allows network monitoring and control.
6. Select **Install OpenSSH** to install [OpenSSH](#) on Windows managed systems.
7. Select **Install the Version Control Agent for Windows (VCA)** to install the HP VCA on Windows managed systems. The HP VCA enables you to view the HP software installed on a system and whether updates for the software are available in the repository.

Installs the HP VCA in conjunction with the Version Control Repository Manager and enables management of the HP ProLiant software and firmware on the managed systems.

8. Select **Register VM Host** for VMware ESX, Citrix XenServer, Microsoft Hyper-V, and Xen on SLES and RHEL (**Register VM Host** is not available for standalone HP SIM).
9. For selected installs, perform the following steps:
 - a. If you are installing software that is earlier than or the same version currently installed, select **Force install the agents**. This option is disabled by default.
 - b. If you want to reboot after the installation, select **Reboot systems if necessary after successful install** option.

HP SIM determines the type of agent or provider to install based on the system type, subtype, and operating system description of the system.

If you want to install a 64-bit agent or provider, be sure the target system is identified as a 64-bit system in HP SIM.

If your system is not correctly identified, go to **System Page**→**Tools & Links**→**Edit System Properties**. Select the correct system type, or subtype and enter the operating system description manually.

Example: Installing Insight Management Agents on a ProLiant Windows 64-bit system:

- a. Select **System type: server**.
- b. Select **System subtype 1: HP ProLiant**.
- c. Enter operating system description as Microsoft Windows Server 2003, x64 Enterprise Edition Service Pack 1 or the correct operating system description of your system.

If you want to configure the agents after installation, select the force reboot option. This allows the newly installed component to be completely initialized before you configure it.

NOTE: Installation with reboot typically takes about 8 minutes.

10. Click **Next**. The **Step 3: Configure or Repair Agents Settings** page appears.

NOTE: The Step 3: Configure or Repair Settings page changes to show the configuration options available with the installed plug-ins.

11. Configure the target systems by selecting one of the following options:

- **Configure WBEM / WMI.** This section enables you to configure the target Linux, Windows, or HP-UX system to send WBEM indications or events to HP SIM.

For this section, consider the following:

- **Create subscription to WBEM events so that WBEM events will be sent to the CMS**
- **Send a sample WBEM / WMI indication to this instance of HP SIM to test that events appear in HP SIM in the Event List or All Event User Interface for the selected system**

NOTE: This indication will appear as an **Informational Event** in the **Event List** of HP SIM.

NOTE: This indication is supported only on HP-UX and Windows targets with WBEM provider installed.

- **Use an HP SIM WBEM certificate (good for 10 years) rather than username/password to manage the system**

This option deploys a WBEM certificate to the managed system and is only valid for HP-UX systems.

- **Configure a non-administrative account for HP SIM to access WMI data**

This option applies to Windows systems with HP WBEM providers. The configuration of the managed system updates to allow the specified user to access WMI information over the network. HP SIM uses this user to read inventory and configuration information from the system and is configured as the WBEM user in the System Credentials. If HP SIM is configured with a user with administration rights, this configuration step is not necessary. HP SIM does not create this user. The user already exists as either a domain user or one local to the managed system.

The user is added to the DCOM Users group on the managed system and has read-only access to WMI information, and read-write permissions to the HPQ name space. This user does not need to be an administrator of the managed system or have sign-in rights. The domain administrator should create a special domain account.

To enter the credentials for HP SIM to use to access the managed systems:

1. In the **User name** field, enter a user name.
2. In the **Password** field, enter the password.
3. In the **Password (Verify)** field, re-enter the password exactly as it was entered in the **Password** field.
4. In the **Domain (Optional)** field, if the target belongs to a Domain, enter the Windows domain.

If configuration of a nonadministrative user is successful, then these credentials are saved as the System Credentials for WBEM access in HP SIM.

- **Configure SNMP**

This section enables you to configure [SNMP](#) settings.

- a. Select **Set SNMP community strings** to specify the Read Community string and the Trap Community string. By default, the first HP SIM read community string that is not public appears. If no community string exists in HP SIM, you must enter one.

NOTE: If you configure only HP-UX systems with default SNMP installations, you do not need to set this option. HP-UX enables read by default (get-community-name is set to public by default on HP-UX systems).

NOTE: If you select this option, the **Read Only** community string is added to the target systems. If the target system is SuSE Linux or Microsoft Windows 2003, the managed systems do not always enable SNMP communication between themselves and a remote host. This setting is modified to enable the instance of the HP SIM system to communicate using SNMP with these target systems.

NOTE: You can enter a community string up to 255 characters.

NOTE: Repairing the SNMP settings adds a **Read Write** community string to the target system only if one does not currently exist. This community string is unique for each system, is composed of over 30 characters to include letters and numbers, and is visible only to the user with administrator privileges for that system. This **Read Write** community string is required by the Web Agent to perform certain threshold setting capabilities. This community string is used locally only on the target system and is not used by HP SIM over the network. Linux and HP-UX systems do not require a **Read Write** community string. The **Read Write** community string is added on Windows systems only.

- b. Select **Set traps to refer to this instance of HP Systems Insight Manager** in the target systems **SNMP Trap Destination List**. This setting enables the target systems to send **SNMP traps** to this instance of HP SIM.

Select **Set additional list of SNMP Trap Destinations for an iLO Management Engine** to set additional SNMP trap destinations. Enter the trap destination information in the fields provided.

- c. Select **Send a sample SNMP trap to this instance of the HP SIM to test that events appear in HP SIM event lists** to verify that SNMP events appear in the HP SIM events list.

To successfully send a test trap, you must configure target systems to send a trap to this instance.

NOTE: You can send a test trap only from a managed system with an Insight Management Advisor installed.

NOTE: The trap from Windows appears as a Generic Trap from the system and is listed as a **Major Event** in the **Event List** of HP SIM. The trap received from Linux and HP-UX targets appears as a Cold Trap and is listed as **Informational Events** in the **Event List** of HP SIM.

- 1) In the **Configure SNMP for iLO Management Engine** dropdown list, select either **Agentless Management** or **SNMP Pass-thru**.
 - 2) In the **Forward Insight Management Agent SNMP Alerts** dropdown list, select either **Enable** or **Disable**.
 - 3) In the **iLO SNMP Alerts** dropdown list, select either **Enable** or **Disable**.
- **Configure secure shell (SSH) access authentication**

Select this option to configure SSH access authentication on managed systems. If you select this option, you must select one of the following options:

 - **Host based authentication for SSH**

NOTE: For this option to work, the user name and password provided in **Step 4: Enter credentials** must be an administrative level account. For Linux or HP-UX targets, it must be the root account and password.

- **Each user has to be authenticated on the managed system**

NOTE: If you do not want all users that have sign-in access to HP SIM to run the tool and you would like to control which users need to have access, this option is more secure.

NOTE: You can configure SSH only if the OpenSSH service is running on the managed systems. You can install OpenSSH on Windows systems by running the **Install Open SSH** or by selecting the tool under **Deploy→Deploy Drivers, Firmware and Agents→Install Open SSH**.

- **Set Trust relationship to "Trust by Certificate"**

Select this option to configure systems to use the **Trust by Certificate** trust relationship with the HP SIM.

For HP SIM on the target systems, this option sets the trust mode to **Trust by Certificate** and copies the HP SIM system certificate to the target system trusted certificate directory. This option enables HP SIM users to connect to the HP SMH using the certificate for authentication.

You can configure SSO to management processors for Onboard Administrator and for remote management. To configure SSO, select **Set Trust Relationship**. After you configure SSO, you are not continually prompted to supply the login credentials for the management processor.

NOTE: For systems with Management HTTP Server 5.x and earlier, the Configure or Repair Agents setting adds the Administrator password in the Management HTTP Server store and modifies the SNMP settings, but it cannot change trust relationship information.

Select the checkbox beside **Import Secure Sockets Layer (SSL) certificate** for HP SIM to trust the HP SMH of the managed system. This option is only valid for HP-UX and Linux operating systems.

- **Configure HP Version Control Agent**

Select this option to configure the HP VCA to point to the Version Control Repository Manager, where the repository of software and firmware is located, enabling version comparison and software updates. This option is available for Windows and Linux systems.

To configure HP VCA:

1. In the **Select the system where the HP VCRM is installed** field, select a server from the dropdown list.
2. In the **User Name** field, enter the user name to access the HP VCRM. This user cannot be the default administrator user, and must have administrative privileges.
3. In the **Password** field, enter the password to access the HP VCRM.
4. In the **Password (verify)** field, re-enter the password for the HP VCRM.

- **Set administrator password for Insight Management Agents version 7.1 or earlier**

Select this option to repair the administrator password on all Insight Management Agents installed on the target systems as applicable for Windows and Linux systems.

NOTE: Do not set this option if you have Insight Management Agents 7.2 or later installed.

NOTE: If the remote system is running HP-UX, this option is not executed on the remote system because it is not applicable on HP-UX systems. If you are configuring only HP-UX target systems, you do not need to set this option.

If you select this option, you must complete the following steps:

- a. In the **Password** field, enter the new administrator password.
- b. In the **Password (verify)** field, re-enter the new administrator password.

Alternatively, select the **Use certificate to authenticate HP Version Control Agent to access HP Version Control Repository Manager** option from **To configure VCRM using certificate** section.

- Select **Configure Insight Remote Support Advanced Settings for iLO Management Engine** to configure Insight Remote Support Advanced settings. Select one of the following options:
 1. Select **Connect this server to an Insight Remote Support hosting server** and enter the Remote Support URL and port.
 2. Select **Disable the Insight Remote Support Advanced connection**.
12. Click **Next**. The **Step 4: Enter credentials** page appears.
 13. Enter the following credentials.

The credentials used in this step must work for all selected target systems. HP recommends using domain **administrator** credentials. Credentials entered here are not saved by HP SIM except to run a scheduled task later.

If you select **Configure secure shell (SSH) access** for a Windows target system, the account you specify must be a member of the local Administrators group. For Windows targets using a domain account, the account is automatically added to this group.

- a. Select one of the following options:
 - **Use sign-in credentials** These credentials must be a privileged account on the managed system. The sign-in credentials option is available if the following options are selected:
 - Install WBEM/WMI Provider (HP Insight Management WBEM Provider) for Windows
 - Install [Simple Network Management Protocol](#) Agent (HP Insight Management Agents) for Windows
 - Install Linux PSP or ESX Agents
 - Install the HP Version Control Agent for Windows

NOTE: This option is not available if you selected **Install Open SSH** or **Register VM Host** on the Step 2: Install Providers and Agents (Optional) page.

- **Use the following credentials for all systems.**
- b. In the **User name** field, enter the system administrator name.
 - c. In the **Password** field, enter the system administrator password.
 - d. In the **Password (Verify)** field, re-enter the system administrator password.
 - e. In the **Domain (Optional)** field, if you are using a domain account, enter the Windows domain.

14. Click **Run Now** or click **Schedule** to run this task at a later time. The **Task Results** page appears. If the Management HTTP Server is installed on target systems, the login credentials are updated in the Management HTTP Server password file. As with other HP SIM tools, you can configure the Configure or Repair Agents tool to run on a schedule or manually. Only one instance of Configure or Repair Agents tool can run at a time.

The Configure or Repair Agents tool can update multiple target systems. The log results indicate whether the repair attempt was successful. For Configure or Repair Agents, the Task Results page displays the following information.

Table 2 CRA Task Results information

Field Name	Description
Status	This field displays the details for each target system within a task instance.
Exit Code	This field represents the success or failure of an executable program. If the return value is zero or a positive value, the executable ran successfully. If a negative value is returned, the executable failed. This exit code does not indicate that all configuration attempts were successful. It is possible for some to succeed but some to fail.
Target Name	This field displays the name/IP address of the target.
The stdout tab	This tab displays the output text information.
The stderr tab	This tab displays information if the executable experienced an error.
View Printable Report When clicked View Printable report, the report gets opened in a new window with only Print link present on it. There are no any Message box , or a OK button present.	You can print reports for the selected target system or for all target systems associated with the task instance. To print a report: - Click View Printable Report. The reports opens in a separate window. Options Message box appears. - Click Print to print the report. - Click the red x on the window to close the report.

Setting up HP-UX servers to be managed by HP SIM

Procedure 3 Setting up HP-UX managed systems

1. Understand the basic managed system software for HP-UX.

For HP-UX, the following software, shown with minimum recommended versions, is required for essential HP SIM functionality to operate. This software is installed by default as part of the latest HP-UX 11i v2 and 11i V3 operating environments, but it might need to be installed or updated on HP-UX 11i v1 or older HP-UX 11i v2 environments.

- T1471AA HP-UX Secure Shell
- B8465BA HP [WBEM Services](#) for HP-UX
- OpenSSL

This WBEM Services bundle contains basic system instrumentation displayed in the HP SIM **Property** pages, supporting collection and reporting by HP SIM inventory functionality. To maximize the value of HP SIM for properties, inventory, and events, see <http://www.hp.com/go/hpsim/providers> for the latest WBEM Services bundle.

If iCap information is desired, also install:

- B9073BA version 08.01.01 iCAP for HP-UX

2. Ensure the managed system software is installed.

To verify that the minimum required software is installed, log in to the remote system, and run the following command:

```
$ swlist -l bundle T1471AA B8465BA OpenSSL
```

To verify that the optional providers and System Management Homepage are installed, run commands such as:

```
$ swlist -l bundle LVMPProvider WBEMP-LAN-00 SysMgmtWeb SysFaultMgmt  
OnlineDiag
```

3. Acquire and install the managed system software if not previously installed.

The SSH and WBEM bundles are included on the HP-UX Operating Environment and Application Release media, as well as part of the HP SIM HP-UX depot downloaded from http://h18013.www1.hp.com/products/servers/management/hpsim/dl_hpux.html.

For the WBEM providers, see http://h18013.www1.hp.com/products/servers/management/hpsim/dl_hpux.html.

After you have obtained the depots containing the software, you can install then from the managed system:

```
$ swinstall -s <depot_location> OpenSSL
```

NOTE: B8465BA and B9073BA version 08.01.01 depends on OpenSSL, so you must install OpenSSL first.

```
$ swinstall -s <depot_location> T1471AA
```

```
$ swinstall -s <depot_location> B8465BA
```

```
$ swinstall -s <depot_location> <names of WBEM providers being  
installed>
```

After you have verified that the correct management software is installed on your managed systems, continue to Chapter 4 “[Credentials](#)” (page 35) to finish the configuration from the HP SIM user interface.

Manually setting up an HP-UX managed system

Although chapters 4-7 explain how to finish configuring managed systems from the HP SIM GUI, this section describes how to perform some of these same steps from the command line for HP-UX systems. You do need to first supply credentials and discover the systems, as described in Chapter 4 “Credentials” (page 35) and Chapter 6 “Discovery” (page 38). Then you can do the following actions from the command line, if desired.

You can use the HP SIM Configure or Repair Agents tool to configure HP-UX managed systems simultaneously, or you can configure each managed system manually.

Configuring SNMP to send traps to the CMS

- On the managed system, add the full host name or IP address of the CMS as a trapdest in the following file:

```
/etc/SnmpAgent.d/snmpd.conf
```

```
trap-dest: hostname_or_ip_address
```

- Stop the SNMP Master agent and all subagents with the command:

```
/sbin/init.d/SnmpMaster stop
```
- Restart the SNMP Master agent and all subagents with the command:

```
/usr/sbin/snmpd
```

Configuring SSH access

On the CMS, copy the SSH-generated public key from the CMS to the managed system using the `mxagentconfig`:

Use one of the following commands:

- `mxagentconfig -a -n <hostname> -u root -f <file_with_root_password>`
- `mxagentconfig -a -n <hostname> -u root -p <root_password>`

NOTE: Using the `-p` option exposes the password through `ps` output, so using the `-f` option (with a file only readable by root, and containing only the managed system root password) is highly recommended when using `mxagentconfig -a`. If you use the `-p` option, enclose the password in single quotes if the password has any special characters, such as `&` or `$`. For more information and options, see the `mxagentconfig` manpage with `man mxagentconfig`.

Subscribing to WBEM indications/events:

NOTE: For more information about HP-UX WBEM events, see the HP SIM online help.

Procedure 4 Subscribing to WBEM indications/events

1. From the managed system, be sure WBEM is installed.

```
swlist -l bundle B8465BA
```

2. Verify that **SysFaultMgmt** provider is installed.

Depending on the System Fault Manager configuration, run the following:

```
cimprovider -lm SFMProviderModule
```

The EMSWrapperProvider appears.

or

```
cimprovider -ls
```

The EMSWrapperProvider appears.

NOTE: For more information regarding System Fault Manager, see [HP System Fault Management Diagnostics](#).

3. From the CMS:

To subscribe to WBEM Events, you must have root access. You can verify what credentials are used for WBEM access by running the following command line:

```
mxnodesecurity -l -p wbem -n <systemname>
```

If the managed system does not have a root level user credential configured, you can add it for the individual system.

NOTE: You can use the Configure or Repair Agents tool in the HP SIM UI to perform this step without permanently recording a **root** password.

- To change the individual system:

```
mxnodesecurity -a -p WBEM -c \  
  <username:password> -n <systemname>
```

4. From the CMS, run the WBEM Indications/Events command line:

```
mxwbemsub -l -n <systemname>
```

For more information on subscribing and unsubscribing to WBEM indications, see the HP SIM online help.

Setting up Linux servers to be managed by HP SIM

To be fully managed by HP SIM, HP ProLiant servers running Linux should have the Insight Management Advisor installed. These agents are part of the ProLiant Support Pack. You can install the ProLiant Support Pack manually, or configure it to be installed as part of your normal operating system deployment procedures.

After setting up the management agents on the managed systems, the rest of the configuration can be done from the HP SIM UI. Continue to Chapter 4 “[Credentials](#)” (page 35) for further information.

Configuring agents remotely using Configure or Repair Agents:

1. For Linux systems, select **Install Linux PSP or ESX Agents**.
2. Click **Next**. The **Step 3: Configure or Repair Agents** page appears.

Manually setting up Linux managed systems

Although chapters 4-7 explain how to finish configuring managed systems from the HP SIM GUI, this section describes how to perform some of these same steps from the command line for Linux systems. You do need to first supply credentials and discover the systems, as described in chapters 4 and 6. Then you can do the following actions from the command line, if desired.

Installing and configuring SSH

Procedure 5 Installing and configuring SSH on a Linux system

1. Verify that SSH is installed on the managed system:

```
rpm -qa | grep ssh
```

If SSH is not installed, see your Linux provider for information about installing SSH.
 2. On the CMS, copy the SSH-generated public key from the CMS to the managed system, and place it in the authorized keys file of the execute-as user (root or administrator).
-
- ❗ **IMPORTANT:** On a non-English CMS, ensure that an administrator account exists on the CMS, and that `mxagentconfig` has run on the CMS for the created administrator account.
- Launch the **Manage SSH Keys** dialog box from the CMS command prompt:

```
mxagentconfig -a -n hostname -u username -p Password
```

Configuring a Linux system to send SNMP traps

NOTE: These steps might vary slightly, depending on your version of Linux. See your Linux provider for details if these file paths and file names do not exist on your system.

Procedure 6 Configuring a Linux system to send SNMP traps

1. Verify that SNMP is installed:

```
rpm -qa | grep snmp
```

If it is not installed, see your Linux provider for information about installing SNMP.
2. If the HP Server and Management Drivers and Agents daemons are installed on your system, stop them:

```
/etc/init.d/hpasm stop
```
3. Stop the SNMP daemon:

```
/etc/init.d/snmpd stop
```
4. Edit the `snmpd.conf` file.

For Red Hat Linux, open the following file in the vi editor:

```
vi /etc/snmp/snmpd.conf
```

For SuSE SLES 8, open the following file in the vi editor:

```
vi /usr/share/snmp/snmpd.conf
```

 - a. Remove the comment symbol (#) from the trapsink line, and add the IP address of the CMS:

```
trapsink IPaddress community
```

where *IPaddress* is the IP address of the CMS.
 - b. Add the CMS to the read only community by adding the line:

```
rocommunity CommunityName IPaddress
```

where *CommunityName* is the SNMP community string used by the CMS and *IPaddress* is the IP address of the CMS.
 - c. Save the changes to the file. To save and close this file using the vi editor, press the **Esc** key, enter `:wq!`, and then press the **Enter** key.
5. Start the SNMP daemon:

```
/etc/init.d/snmpd start
```

6. If the HP Server Management Drivers and Agents daemons are installed on your system, start them:

```
/etc/init.d/hpasm start
```

4 Credentials

In HP SIM, credentials are used to enable the CMS to communicate with managed systems, through WBEM/WMI, WS-MAN, SSH, SNMP, and SNMPv3. However, the Sign-in credential is used unless you configure the other protocols. The Sign-in credential is protocol independent and can be tied to systems through the discovery credential. In HP SIM, there are three different types of credentials:

- **System credentials**

Credentials used by [identification](#) to access managed systems. These credentials include WBEM/WMI, WS-MAN, and SSH credentials, Sign-in, SNMP community string, SNMPv3, and [Single Sign-On](#) (SSO) credentials.

- **Discovery task credentials**

Credentials used by a discovery task that apply to all systems discovered by that task.

- **Global Credentials**

Global credentials are system credentials that apply to all systems.

During the identification process (done automatically during discovery), credentials are tried, starting with System Credentials. If they do not work, and the **Try Others** setting is chosen for them, then Discovery credentials are used. Similarly, if those do not work and the **Try Others** setting is chosen, then Global Credentials are tried. As soon as a credential is found that works, HP SIM notes that credential as *working* and continues to use it for regular communications with the managed system as long as it continues to work. If it should fail, then the process is repeated the next time identification is run. To see the *working* credentials for any managed system, go to the **System Credentials** page (**Options**→**Security**→**Credentials**→**System Credentials**). These *working* credentials appear in the **Credentials that are in use** table.

When a discovery credential is used to successfully communicate with a system, a credential reference is created for that system. If the credential is later changed on that same discovery task, the credential that is used on all systems referencing it changes. This enables credentials to be changed in one place (usually passwords for an account) and immediately be available for use in HP SIM. The same is true for global credentials.

Because of this, if a global or discovery credential is deleted, you are asked if all references to that credential should be removed or if copies should be made as system credentials for each system that is referencing the current credential.

However, when a credential is overwritten, instead of deleted and then re-added, the credential is changed and each system referencing it uses the new username/password values.

If the intent is not to change what is currently in use, you must add a new credential. For discovery tasks, a new discovery task must be created with its own credentials, instead of editing an existing discovery task, if the systems require different credentials than contained in the existing discovery task.

Example XML file to add more than 10 WBEM username and password pairs

To save time and effort, create an XML file that defines your system authorizations before running discovery. For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
15.43.215.47
```

```

15.43.212.150
15.3.110.117
15.3.105.51
15.3.110.113
-->
<nodelist>
<node name="system1">
<credential protocol="wbem" username="root "
password="pswd" />
</node>
<node name="system2">
<credential protocol="wbem" username="root "
password="pswd" />
</node>
<node name="system3">
<credential protocol="wbem" username="root "
password="pswd" />
</node>
<node name="system4">
<credential protocol="wbem" username="root "
password="pswd" />
</node>
<node name="system5">
<credential protocol="wbem" username="euploid\administrator"
password="pswd" />
</node>
</nodelist>

```

You can include the IP addresses of the systems to be discovered in an XML comment so that you can maintain the IP addresses with the XML file and can copy and paste into the **Ping inclusion ranges, system (hosts) names, templates, and/or hosts files** field when creating or editing a discovery task.

After you create the XML file import it into HP SIM before running discovery using the following CLI command:

```
mxnodesecurity -a -f <path-to-xml-file>
```

HP recommends limiting the WBEM user name and password pairs to 10 to reduce the overall discovery run time.

5 WMI Mapper Proxy

Windows systems use a variation on the WBEM [management protocol](#) called WMI. For HP SIM to communicate with Windows systems, the WBEM protocol it uses must be converted to the WMI protocol and vice versa. This is the function of the WMI Mapper Proxy. This proxy is typically installed on the same system as HP SIM when HP SIM is installed on a Windows system. For Linux or HP-UX installations where Windows systems will be managed, it can be installed on a separate Windows system, with its location configured in the **Options→Protocol Settings→WMI Mapper Proxy** menu.

You can configure the WMI Mapper Proxy from the First Time Wizard. You can also add, edit, and delete WMI Mapper Proxies by selecting **Options→Protocol Settings→WMI Mapper Proxy**.

6 Discovery

Discovery is the process of finding systems in the [management domain](#) so that they can be managed from the CMS by HP SIM. HP SIM can automatically discover and identify systems attached to the network using information from management protocols such as SNMP, SNMPv3, WMI, WBEM, SSH, and SSL. Create discovery tasks to limit discovery to specific network segments or IP address ranges, or to control the frequency that each task runs. Use discovery filters to prevent discovery of unwanted system types.

When you access the **Discovery** page, a table displays a list of all available discovery tasks. You can configure multiple instances of discovery with each instance having its own schedule and set of inclusion ranges. When a discovery task is executed, the **Last Run** column is updated to display its progress, including the percentage of completion.

Automatic discovery and completion percentages are calculated by weighting two factors: the ping sweep (performed on each host) is 10% of the process; the system identification is 90% of the process. If no host is found on an IP address, the system identification is considered complete. For example, you have 100 hosts in your discovery range. If 50 hosts have been pinged, but only 10 identified, you have: $50/100 * .10 = 0.05$ (ping sweep) $10/100 * .90 = 0.09$ (identification) $0.05 + 0.09 = 0.14 * 100 = 14\%$ (total completed percentage).

NOTE: You can run only one discovery task at a time. If you select to run more than one discovery task, the percentage in the **Last Run** column remains at 0% until the currently running task is complete.

When multiple Command View (CV) consoles are discovered in HP SIM, with each actively managing its own EVAs, the managed system section of the CVEVA listing in HP SIM displays all of the Storage Arrays (both actively managed and passively managed).

When another CVEVA server is discovered in HP SIM, which is managing the same set of Storage Arrays, the managed system section of both CVEVA servers display only arrays managed actively.

Recommended discovery tasks

For best results, HP recommends creating the following discovery tasks, and running them sequentially in the suggested order. You might want to create multiple tasks for certain types, such as servers, grouping them so that systems with the same credentials are in the same discovery tasks, with up to three sets of credentials supplied in each discovery task. This reduces the chance of account lockout when an invalid credential is tried too many times.

1. Central Management Server (CMS)

This discovery task is for discovery of the HP SIM CMS and its management processor, if it has one.

2. Onboard Administrator

This discovery task is for discovery of the Onboard Administrators for every enclosure to be managed. When specifying credentials for this task, include the iLO credentials for every blade in the enclosures associated with the Onboard Administrators.

3. Management Processors

This discovery task is for discovery of all management processors not discovered in the previous tasks. This includes iLOs and management processors for all non-blade systems.

4. Physical Servers

This discovery task is for discovery of physical servers (blade servers and standalone servers). The management processors for these servers must be discovered prior to this discovery task being run.

5. Virtual Machines

This discovery task is for discovery of virtual machines associated with servers discovered in the previous category.

NOTE: If discovery tasks are run out of order, errors are likely. Typical errors due to running discovery tasks in an improper order include:

- **Association errors**

For example, a server not associated with a management processor or virtual machine not associated with a virtual machine host.

- **Credentials errors**

Because discovery of systems can trigger additional discovery of associated systems or management processors, if the correct credentials are not supplied for the associated systems, their discoveries are likely to show errors. If you discover these associated systems with a subsequent discovery task containing the proper credentials, they should then complete successfully.

NOTE: Citrix Xen VMs discovered in category 5 will always return a discovery error unless the Citrix Xen Host has been registered through **Configure**→**Virtual Machine**→**Register Virtual Machine Host**.

If you have a small network, an alternate way of setting up your discovery tasks is to create a single task with one IP address range and all of the required credentials for the systems in that range. However, doing this can make it difficult to troubleshoot and diagnose errors if one or more systems are not configured correctly.

Options on the Discovery page

Under the **For all automatic discoveries** section, the following options are available:

- **Configure general settings**

Select this option to configure general settings that apply to all discovery tasks.

- **Manage hosts files**

Select this option to manage [hosts files](#)

- **Configure global protocol settings**

Select this option to configure global protocol settings.

NOTE: To discover clusters correctly, you must enable SNMP with the correct security settings on HP SIM on the target systems.

From the **Discovery** page, you can:

- **Create a new discovery task**

Click **New** and the **New Discovery** section appears.

- **Edit an existing discovery task**

Select a task from the table, and click **Edit**. The **Edit Discovery** section appears.

- **Enable or disable a discovery task**

Select a task and click **Disable** to disable the schedule of an enabled task. If a task is disabled, the button changes to **Enable**. To resume automatic execution of the task, click **Enable**.

- **Delete an existing discovery task**

Select a task from the table and click **Delete**.

- **View Task Results**

This button displays the task results for the current discovery task.

- **Run a discovery task**

Select the task you want to run and click **Run Now**. When a task is running, the **Run Now** button changes to a **Stop** button.

- **Stop a discovery task from running**

Select the running task and click **Stop**.

See the Systems Insight Manager online help for more information on each of these options.

Discovery credentials

One of the best ways to configure credentials for your managed systems is to do so as part of a discovery task. You can enter one or more sets of credentials. As each system is discovered, the credentials listed in the discovery task will be tried on it, in order, until one set is found to work. This set will be saved as the working credentials for that system. You can configure more than one set of credentials for each discovery task, but it is suggested that you keep it to a small number (less than 5) for best performance. If possible, group systems with similar credentials into the same discovery task.

Configuring Configure or Repair Agents through a discovery task

You can choose to have additional configuration done on the managed systems, as they are discovered, by configuring the settings using the Configure or Repair Agents button. For additional information, see the HP SIM online help.

Viewing discovery task results

To display the task results for discovery task, select the task on the **Discovery** page, and then click **View Task Results**. You can also view discovery task results, by selecting **Tasks & Logs**→**View Task Results**.

Discovery filters

Discovery filters prevent or enable certain system types from being added to the database through automatic discovery. When you want to discover systems of a certain type, using filters is much easier than specifying the IP addresses of each individual system. Discovery filters do not apply to individually added systems.

You can access discovery filters from the **Discovery** page by selecting **Enable discovery filters** in the **Configure general settings**, section.

To disable filters, clear the **Enable discovery filters** checkbox. To enable filters, select the **Enable discovery filters** checkbox, and then select the system types that you want to discover.

To access and modify discovery filters, you must have [administrative rights](#). If discovery filters are enabled, only systems of the selected types are added to the database through automatic discovery. Because all [tasks](#) operate on systems that exist in the database, tasks do not run on any system until the filter criteria has been met and that system has been added to the database. Filters do not affect any systems already discovered, even if the systems change to a type that no longer

matches the current filter. If discovery filters are disabled, automatic discovery discovers systems according to the **General Settings for All Discoveries** section on the **Discovery** page.

If you do not discover the HP systems that you expect to find, ensure that the HP Insight Management Advisor are installed and running correctly on the target systems. In addition, verify that the SNMP Community Strings settings and WBEM user name and passwords in HP SIM and on the agents for systems that are not discovered are configured correctly.

Discovery of Gen8 servers

Discovery for a Gen8 server must happen through the IP address of the host server's iLO4 IP address. If it is a blade server, you can discover the server through the Onboard Administrator IP address. If the host IP address is used, it will be discovered, but will not include all the HP Management Instrumentation, as this now all comes from the iLO4. It is the iLO4 which makes all the proper associations (along with Onboard Administrator if it's a blade). The host is fully off loaded from the system management tasks.

Discovery for the Gen8 with host-based agents fully installed, properly configured, and agentless mode disabled, can be discovered through a number of ways. This host IP is the correct place to find all you would need. Additionally, an Onboard Administrator IP if the host is a blade, is also allowed here. Since this is using host-based agents, the iLO4 can be viewed as a pass through to the host, and could be used as well, but is treated as a management processor, not a host NIC.

7 Manage Communications

Use the **Manage Communications** feature to troubleshoot communication problems between the CMS and targeted systems. For each failed communication function, troubleshooting information is available. You can reconfigure communication settings, launch agents, and push certificates to target systems. This feature is available by selecting **Configure→Manage Communications** menu and includes the following tabs:

- **Identification tab**
Includes status information on the state of an identification process . Identification attempts to determine what the system type is, what management protocol a system supports, and attempts to determine the operating system and version loaded, along with other basic attributes about the system. Finally, it determines if the system is associated with another system.
- **Events tab**
Indicates if the CMS can receive events from the target systems. This status considers the setting of SNMP traps and WBEM indications.
- **Run Tools tab**
Indicates if the CMS can run tools locally on target systems. Communication issues in this column usually relate to security and trust relationships.
- **Version Control tab**
Indicates the availability of software and firmware inventory data for target systems. The status is collected and stored during data collection.

The following information is available:

- **Advising and repairing managed system settings**
Includes a tabbed interface with a tab for each functional column (**Identification**, **Events**, **Run Tools**, and **Version Control**). Each tab displays the diagnostic results and includes troubleshooting tips and advice for fixing communication problems.
- **Quick repairing managed system settings**
Launches the Configure or Repair Agents tool. Configure or Repair Agents enables you to quickly and optimally configure systems for manageability.
- **Updating communication status**
Runs to get an updated communication status.
- **Printing Manage Communications table**
Creates a printer-friendly version of the list in a new window.

NOTE: Experienced users who do not need the troubleshooting advice might be able to repair their systems faster with the Configure or Repair Agents feature. To access Configure or Repair Agents, select **Configure→Configure or Repair Agents**.

Configuring the managed system software using the Configure or Repair Agents feature from the CMS

The HP SIM Configure or Repair Agents tool is a quick and easy way to configure Linux, HP-UX and Windows managed systems to communicate with HP SIM.

To run Configure or Repair Agents remotely against multiple systems simultaneously, you must have authorizations to run the Configure or Repair Agents tool.

In addition, you must enter administrator level user credentials for the target system.

Sending test traps and indications

To verify that SNMP traps and WBEM indications can be sent, send test traps and indications.

You can send test traps and indications from Configure or Repair Agents on Windows and HP-UX systems, with the WBEM provider installed, from the **Step 4: Configure or Repair Agents** page, under **Configure WBEM / WMI**.. Select **Send a sample WBEM / WMI indication to this instance of HP SIM to test that events appear in HP SIM in the Event list or All Event User Interface for the selected system**..

You can also send test WBEM indications from some HP-UX version by running the following procedure:

Procedure 7 Sending WBEM indications From an HP-UX system

1. From the HP-UX managed system, run `/ect/opt/resmon/sbin/send_test_event monitor name` . For example, `/etc/opt/resmon/sbin/send_test_event disk_em`.

Possible monitor names:

- dm_memory
- lpmc_em
- disk_em
- dm_chassis
- dm_core_hw
- ia64_corehw
- fpl_em

2. Confirm that the test indication is shown in the HP SIM event table view after you trigger it.

Procedure 8 Sending WBEM indications from a Windows system

1. Login to the target Windows system.
2. Go to **Start→Programs→HP Insight WBEM Providers→Test WMI events**.
3. Click any one of the severities (Informational, Warning, or Error).
4. Click **OK** to send the test events to the CMS.

Procedure 9 Sending SNMP traps from Windows or HP-UX system

1. Run Configure or Repair Agents and on **Step 4: Configure or Repair Agents** under **Configure**, select **Send a sample SNMP trap to this instance of HP SIM to test that events appear in HP SIM in the Event list or All Event User Interface for the selected system**.
2. Confirm that the test trap is shown in the HP SIM event table view after you trigger it.

8 Automatic event handling

Automatic event handling enables you to define an action that HP SIM performs when an event is received. Users who want to access this feature must have [administrative rights](#).

NOTE: Automatic Event Handling events older than 24 hours are filtered out from AEH tasks.

- **Creating a New Task**

Enables you to create a new Automatic Event Handling task. Select **Options→Events→Automatic Event Handling→New Task**.

- **Managing Tasks**

Enables you to view definitions, copy tasks, edit tasks, view task results, disable or enable tasks, or delete existing Automatic Event Handling tasks. Select **Options→Events→Automatic Event Handling→Manage Tasks**

- **E-mail Settings**

Enables you to set up the various e-mail settings needed because of an event action. You can access the **E-mail Settings** page using one of the following methods:

- Select **Options→Events→Automatic Event Handling→E-mail Settings**.
- From the HP SIM introductory page, click **e-mail** in the **Do this now to finish the installation** section.

E-mails are sent to alert users about problems. Ask your e-mail administrator to verify whether you need the following information:

- SMTP host name of the outgoing mail server, such as *mail.company.com*. This server receives the mail messages from HP SIM and begins routing them to the recipient.
- The name of the management server e-mail address. This address appears in the **From** field of any e-mail sent from HP SIM. The user can be a system name. Enter the full domain address in the form *server@domain.com*, as the sender.

NOTE: Some e-mail systems require a valid From user before they accept the message. HP suggests that a valid e-mail account be used for this purpose.

- **Modem Settings**

Enables you to set up a modem to use for alphanumeric paging. Before you send a page from the HP SIM server, set up the modem on the server. Be sure you know the COM port used by the modem to send the page.

This feature is available to users with [administrative rights](#) only and is available only when the HP SIM CMS is installed on Windows.

You can access the **Modem Settings for Paging** page using one of the following methods:

- Select **Options→Events→Automatic Event Handling→Modem Settings**.
- From the HP SIM introductory page, click **paging** in the **Do this now to finish the installation** section.

Access the **Automatic Event Handling** page to edit or delete an existing rule by clicking **Automatic Event Handling** in the **Do this now to finish the installation** section of the HP SIM introductory page.

Example automatic event handling tasks

HP SIM ships with three example automatic event handling tasks that are disabled by default. When the **Automatic Event Handling - Manage Tasks** page appears, you can select one of the example tasks and click **View Definition**.

- **example - all desktop information events**

This task is triggered when an informational event is received from the discovered desktop systems, and this task clears the event. The same task can be edited to change the action of the system criteria .

- **example - all linux MIB updates**

This task is triggered when a MIB update events request is received from all managed Linux target systems that are discovered and identified in HP SIM. The same task can be edited and saved as new task.

- **example - all server failed sign-in events**

This task is triggered when a failed sign-in attempt is made. Sign-in failure might be caused by an invalid user account, sign-in attempt from an excluded IP address, or failed sign-in authentication.

9 Users and Authorizations

HP SIM enables you to configure authorizations for specific [users](#) or [user groups](#). Authorizations give the user access to view and manage systems. Each authorization specifies a user or user group, a [toolbox](#), and a system or system group. The specific set of tools that can be run on a system is specified in the assigned toolbox.

You must plan which systems each user will manage and which specific set of [tools](#) each user is authorized to execute on managed systems. A user with no toolbox authorizations on a particular system cannot view or manage that system.

Authorizations are cumulative. If a user is authorized for Toolbox1 and Toolbox2 on the same system, the user is authorized for all tools in both Toolbox1 and Toolbox2 on that system. Similarly, a user authorized for the **All Tools** toolbox on a system requires no other toolbox authorizations on that system because the **All Tools** toolbox always includes all tools. See the Systems Insight Manager online help for more information on setting up users and authorizations.

Users

Create user accounts to sign-in to HP SIM. The account must be valid on the operating system (including Active Directory on Windows) on the CMS and is authenticated by the CMS. You must know the operating system [user account](#) name of the user you are adding, but it is not necessary to know the password.

User groups

User groups must exist in the operating system. For Windows, they must also exist in Active Directory. Members of user groups in the operating system can sign-in to HP SIM and inherit the group's attributes for configuration rights, sign-in IP address restrictions, and authorizations. When a group's configuration rights, sign-in IP address restrictions, or authorizations are changed, this change is immediately reflected for all current members of the group.

With configuration rights, the user inherits the highest setting. With sign-in IP address restrictions, the user inherits all entries. With authorizations, the user inherits all authorizations.

NOTE: A user's group membership is determined at sign-in. If a user's group membership changes in the operating system, it is not reflected in HP SIM until the next time the user signs in to HP SIM.

Toolboxes

Toolboxes are used to configure a group of [tools](#) for each [user](#) that has access. Toolboxes are set up so that some users can use the group of tools to which each user has access but not others. For example, an administrator has access to more tools than a user.

NOTE: For users with [operator rights](#) and user rights to clear, delete, assign events, and add comments to events, you must select **Configuration Tool** from the **Show tools in category** dropdown list. Then, select **Clear Events**, **Delete Events**, **Assign Events**, and **Comment Events** as necessary, and then click  to add them to the **Toolbox contents**.

10 Managed environment

The Managed Environment feature enables you to select the operating systems that you will manage. There are four options: Windows, Linux, HP-UX, and Other. The selections made here configure HP SIM to hide collections, tools, and reports for operating systems you do not manage.

NOTE: These settings can be changed at any time, and the hidden collections, tools, and reports can be made visible again.

If you select **Linux** or **HP-UX**, you can select to have GlancePlus or Ignite-UX and Software Distributor menu items appear in HP SIM. The **HP-UX** menu items are for handling Integrity Extensions on a Windows or Linux CMS and are not available on an HP-UX CMS.

If both **Linux** and **HP-UX** are selected, the same user name must be specified for GlancePlus in both the places. Root user is used if no user name is specified.

If you select HP-UX, select **Ignite UX and Software Distributor**, and then enter the IP address of the ignite server and the SSH credentials (Host based or User based).

NOTE: The password field is populated with a dump value, not with the actual password supplied by user. Dump value is used as a security measure. All selections are retained when you move around in the UI. The same selections are retained in **Options→Managed Environment** page.

Part III HP SIM basic features

11 Basic and advanced searches

Basic search

The Search feature enables you to quickly retrieve details about a [system](#) using its name or common system attributes. For example, you could search for a system name, IP address, or a word such as server, HP-UX, or storage.

The search field only allows the following characters: letters, numbers, tilde (~), dash (-), period (.), underscore (_), apostrophe ('), and space.

As you type, a dropdown list appears and lists systems with names that begin with the text entered. The list includes up to 12 systems, and shows the icon for the system health status. If more than 12 systems are found, an ellipsis (...) appears at the bottom of the list. Continue typing to narrow the list further. You can use the mouse or arrow keys to select a system to view, or do not select a system and press **Enter** or click **Search** to search for the indicated criteria.

If you selected a system in the dropdown list, the **System Page** for that system appears.

If you did not select a system, and you pressed **Enter** or clicked **Search**, the **Search Results** page displays a list of systems that match your criteria. Clicking a name in the list displays the **System Page** for that system. If no system in the database resembles the target system, the **Search Results** page indicates that no entries meet the criteria, and gives you the option to search again or perform an advanced search.

Advanced search

To access the **Advanced Search** page, click the **Advanced Search** link in the **Search** panel.

You can create a system, [event](#), or [cluster](#) search by selecting **systems**, **events**, or **clusters** in the **Search for** box at the top of the **Advanced Search** page. Then you can specify the criteria to be used in the search. The result of running a search is a collection. The criteria selected can also be saved as a collection definition, so that search can be run again at a later date. The saved collections are stored in the **System and Event Collections** panel as **Systems** or **Events**. These collections can be saved as private or shared.

Hierarchical displays

Some search criteria require hierarchical displays. Examples of hierarchical criteria are: Operating System, Event Type, and Software/Firmware.

In these cases, the comparison selection box is replaced by a selection box containing the appropriate syntax for that particular tree level. The most complex of these cases is the Software/Firmware criteria. When Software/Firmware is selected, a series of search criteria are added below in a tree format:

- component type is
- and operating system is
- and category type is
- and name is
- and version is

In this case, as selections are made in the higher-level selection boxes, the available selections in lower-level boxes are updated.

Save as

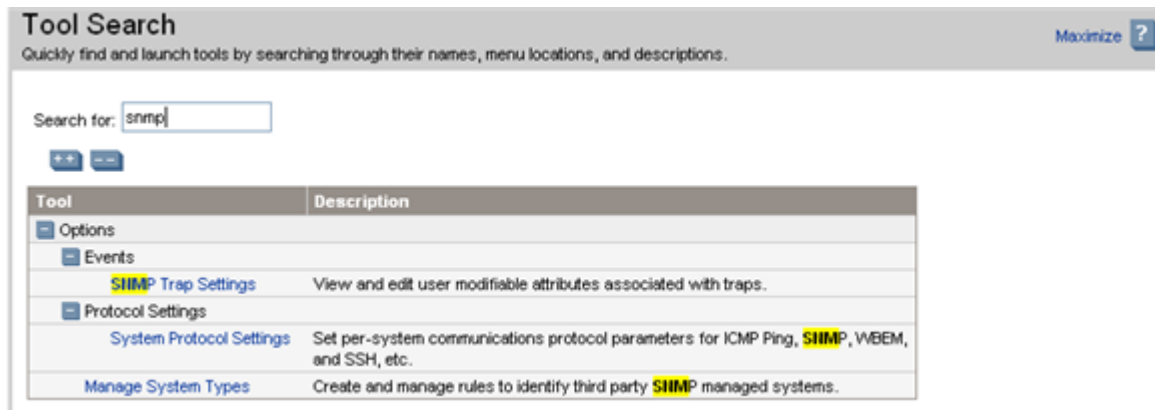
When you click **Save As Collection**, the **Save As Collection** section displays. Enter a name for the search in the **Name** field, and then select where to save it.

View

When you click **View**, the results of the search appear below the search frame. This functionality enables you to preview the results of the search before saving it, or to run a search without saving it.

Searching for tools

The Tool Search feature provides a quick way to search and filter textually, based on tool names, tool locations in the HP SIM cascading menu structure, and tool descriptions.



For additional information, see the HP SIM online help.

12 Monitoring systems

Viewing system collections

In HP SIM monitoring systems involves HP SIM polling [Insight Management Advisor](#) or firmware on the managed systems to retrieve status information, and then displays this information as status icons. There are several types of status that can be displayed, such as Health Status (HW), Software Versioning Status (SW), or Management Processor status (MP). Other status icons might be added by plug-ins to HP SIM. These icons enable you to see, at a glance, the state of your systems.

Pages displaying system status

- **System lists**

There are four system lists page views; table view, icon view, tree view, and picture view (for racks and enclosures). Common in each view is the system name and system status. To access the system list pages, select a collection or system from the **System and Event Collections** panel. The type of collection or system that you select determines the view that appears.

- **Table view**

The **HS** column on the system list page displays the overall [system health status](#), which is determined by the default Hardware Status Polling task and is a roll up of all the status sources, which can be SNMP, WBEM, HTTP, and cluster status. The legend shows how many systems in the view are Critical, Major, Minor, Normal, Disabled, and Unknown.

- **Icon view**

The icon view lists the system name of all discovered systems, as well as the [system health status](#) for each system. The legend shows how many systems in the view are Critical, Major, Minor, Normal, Disabled, and Unknown.

- **Tree view**

The tree view displays the health status icon and the system name for each system in a tree format.

- **Picture view**

The picture view page for racks and enclosures contains a picture view of the discovered systems in the rack or [enclosure](#) if available. While signed in to HP SIM, placing your cursor over a server shown in the view displays information on that particular server, including [server blade](#) name, slot number, and the enclosure in which the server is located. You can also click a component name to display detailed information about the component.

In all views, you can select the checkbox next to the system name to select a system. You can select more than one system, or to select an entire collection, select the checkbox, **Select "collection name" itself**.

- **System pages**

On the **System Page**, **System** tab, a status icon indicates the overall health status stored in the database. If system monitoring is suspended, a disabled icon appears in place of the hardware status icon and software status icon. The **System Status** section contains more information on the [system](#) status.

You can access the **System Page** one of the following ways:

- Select **Tools**→**System Information**→**System Page**, and then select a target system.
 - Click the system name in the **System Name** column on the system table view page.

- **Property pages**

The **Property** page **Status** tab displays WBEM properties that help determine the status of the target system, such as determining memory status and process status. Computer system status is determined by information collected live through the WBEM protocol and the information provided by the WMI provider.

You can access **Property** pages in the following ways:

- From the **System Page** on the **System** tab, click **Properties**. The **Property** pages appear for the target system.
- Select **Tools**→**System Information**→**Properties**, select the target system, and click **Run now**. The **Property** pages display for the target system.

- **System Status Panel**

This panel provides uncleared event status, system health status information, and an alarm to notify you about certain events or statuses. The **System Status** panel is in the upper left corner of the HP SIM GUI and can be customized by clicking the **Customize** link within the panel.

Viewing health status from the table or icon view

To display the next level of status detail from any page in HP SIM that shows a health status icon, place your cursor over the icon and additional status detail information appears. The status values that appear depend on the agents installed on the target system.

In some cases, the system is a container, such as a rack, enclosure, [complex](#), or cluster. In the table and icon views, the status value is the status of the container and does not include status of subsystems. If the status is Unknown, only the system name and Unknown status icon appears.

Viewing health status in the tree view

The tree view displays status data for each system, as well as rollup status for container systems. The status icon is located on the left side of the tree view next to the selection checkbox. For systems that are containers, the status to the left of the container name indicates the most critical status of the systems in the container, including the container status itself. The status of the container itself, if there is one, appears to the right of the system name, inside parentheses, alongside the system type label. Placing your cursor over the status icons will reveal additional status details.

System status types

The following table describes the HP SIM, system health status types, which appear in the **HS** column on the system list page.

Table 3 Health status types

Status icon	Status type	Description
	Critical	HP SIM can no longer communicate with the system. The system was previously discovered but cannot be pinged. The system might be down, powered off, or no longer accessible on the network because of network problems.
	Major	A major problem exists with this system that should be addressed immediately. For systems running Insight Management Agent, a component has failed. The system might no longer be properly functioning and data loss can occur. In Insight Manager (WIN32), this status was identified as <i>Failed</i> .
	Minor	A minor problem exists with this system. For systems running Insight Management Agent, a component has failed, but the system is still functioning. In Insight Manager (WIN32), this status was identified as <i>Degraded</i> .

Table 3 Health status types *(continued)*

Status icon	Status type	Description
	Warning	The system has a potential problem or is in a state that might become a problem.
	Normal	The system is operating normally. The system is accessible.
	Disabled	The system is suspended, which enables a system to be excluded from status polling, identification, data collection, and automatic event handling. On the Automatic Discovery page, if you select the Automatically discover a server blade when its iLO is identified option, new servers discovered through iLO (for example, no operating system or IP address known) are shown as disabled until the system is discovered with an IP address or operating system.
	Unknown	HP SIM cannot obtain management information about the system using SNMP. Although no management instrumentation information is available, the system can be pinged. It might have an invalid community string or security setting, or it might be an IP address that is no longer associated with a system.
	Informational	The system might be in a transitional state or a nonerror state.
	No Status	The system has not been polled by one or more of the polling tasks since the system was discovered.

Software status types

The following table describes HP SIM system software status types, which are displayed in the **SW** column on the system list page.

Table 4 Software status types

Status icon	Status type	Description
	Major	An update that contains a critical bug fix is available for this system.
	Minor	An update that contains new hardware support or bug fixes is available for this system.
	Normal	All components on the system match the repository.
	Disabled	The system is suspended. No software status is available.
	Informational	The CMS could not reach the HP VCA on the system, so the status of the system is unknown.
	Unknown	The HP VCA cannot communicate with HP Version Control Repository Manager (HP VCRM). The Unknown status appears for server systems only under the following circumstances: • The HP VCA is not installed on the managed server. • The HP VCA is installed on a server, but that server does not have a trust relationship established with HP SIM. • The operating system on the target server is not supported. Windows and Linux operating systems are supported. • The correct version of the agent is not on the target system. • The target server type brand is not supported (only HP or Compaq brand servers are supported). • The target system is not licensed for monitoring by the HP Insight Performance Management Pack (PMP). The target system must have the Insight Management Agent 6.20 or later installed. • PMP reports an indeterminate status for the system.

WBEM operational status types

HP SIM reports WBEM operational status for storage and server elements, such as storage switch ports and filled memory slots. These status icons appear on the **Property** pages, **System Page**, and in the status details that appear when you mouseover the health status column on the **System Page**. The following statuses are available:

Table 5 WBEM operational status

Status icon	Status type	Description
	Non-recoverable error, lost communication	HP SIM can no longer communicate with the element. - Nonrecoverable indicates that the element has failed, and recovery is not possible. - Lost communication indicates that the element was previously discovered but is currently unreachable.
	Predictive Failure, Error, Aborted, Supporting Entity in Error	A major problem exists with this system and must be addressed immediately. - Predictive Failure indicates that the element is functioning nominally, but a failure is likely to occur in the near future. - Error indicates that the element is in an error state. - Aborted indicates that the element's functionality has stopped abruptly. The element's configuration might need to be updated. - Supporting Entity in Error indicates that the element might be functioning normally, but an element that it depends on is in an error state.
	Degraded, Stressed	A minor problem exists with this element. - Degraded indicates that the element is not operating at optimal performance or might be reporting recoverable errors. - Stressed indicates that the element is functioning but needs attention.
	Normal	The element is operating normally.
	In service, Stopped	The element is suspended. - In Service indicates that the element is being configured. - Stopped indicates that element is stopped.
	Unknown, No contact	No management information about the element could be obtained. - Unknown indicates that the element status is not available. - No Contact indicates that the element exists, but HP SIM has never been able to communicate with it.
	Starting, Stopping, Dormant, Power Mode, Other	This status provides useful information about the port. No attention is required. - Starting indicates that the element is starting. - Stopping indicates that element is stopping. - Dormant indicates that the element is inactive. - Other indicates that additional information is available, but it does not fit into the previously listed categories.

Monitoring clusters

To access MSCS [Cluster](#) collections in the **System and Event Collections** panel, click **Systems** and then select one of the available cluster collections. [Users](#) with [administrative rights](#) can manage all

shared cluster collections from the cluster collection view. Users can manage their own private collections, as well as:

- **Save collections**

Click **Save As Collection** from the cluster table view page.

- **Delete clusters**

Click **Delete** from the cluster table view page. A confirmation box appears. To delete the cluster, click **OK**, or to cancel the deletion, click **Cancel**.

NOTE: Clusters that contain cluster members cannot be deleted. To delete a cluster with its cluster members, select the **All Systems** collection in the **System and Event Collections** panel. Then, select the cluster and all of its members, and then click **Delete**.

- **Print cluster collection view**

Click **Print** to print the collection results.

- **Customize the view**

Click **Customize** to customize which columns display and in what order.

System properties

The Set System Properties tool enables you to set [system properties](#) for a single system or for multiple systems.

You have two options for setting system properties:

- **Edit system properties for a single system**

Select the **Tools & Links** tab on the **System Page**, and then click the **Edit System Properties** link.

- **Set system properties for one or more systems**

Select **Options**→**System Properties**→**Set System Properties**.

The Suspend or Resume Monitoring tool enables you to suspend monitoring of a single system or multiple systems, which enables systems to be excluded from status polling, identification, data collection, and the automatic event handling features of HP SIM. The available suspend lengths include the predetermined increments of 5 minutes, 15 minutes, 1 hour, 2 hours, 4 hours, 8 hours, 1 day, 2 days, 3 days, 4 days, 5 days, 6 days, and 7 days. You can turn on the suspend tool indefinitely. Configuration changes take effect immediately. To view the new settings for a system, click the **System** tab on the **System Page**. Changes made with this tool override previous settings. A system that is suspended appears with a disabled icon throughout HP SIM.

You can suspend or resume monitoring using one of the following methods:

- **Suspend or resume monitoring for a single system**

Click the **Tools & Links** tab on the **System Page**, and then click the **Suspend/Resume Monitoring** link.

- **Suspend or resume monitoring for one or more systems**

Select **Options**→**System Properties**→**Suspend or Resume Monitoring**.

NOTE: You must have [administrative rights](#) to access these tools.

For ESXi system, the **WBEM Health Inclusion Status** link takes you to the **WBEM Health Inclusion Status** page in HP SIM. From this page, you can disable all or part of the sub-component status for an ESXi system so that they do not affect the overall status of the ESXi system. This is useful to disable disconnected NICs from reporting an error status on the ESXi overall health.

After setting the Ignore status on the components, the change will not be reflected until after the next status polling task runs.

Example of setting system properties

Setting customer company and contact information individually

If the customer company or contact information is different between multiple systems, the preferred configuration method is through the **Set System Properties** or **Edit System Properties** page using the procedures outlined below.

HP SIM provides two sections on the **Set System Properties** page under **Contract and Warranty Information**, called **System Site Information** and **Customer Contact**. Each section is treated by HP SIM as a unique database record with the first field of each section representing the record's header.

The **System Site Information** section uses **Site name** as the header, and **Customer Contact** uses **Contact's first name** and **Contact's last name** as the header. You must be aware, when entering information in these sections, that certain properties are tied to the **Site name** and **Contact's first name / last name** fields. If information is meant to be unique for a particular system or system location, you must ensure that the **Site name** and/or **Contact's first name/last name** are also unique.

Under **Customer Contact**, changing any of the fields **Contact job title** through **Contact other** changes the corresponding properties for *all* of the systems that use the same **Contact's first name/last name**.

For example, if the **Site name** was set globally to *Widgets Inc.* and you require a unique address for an individual system located in Brussels. You can create a **Site name** of *Widgets Inc. — Brussels* to ensure that the unique address information for this system does not overwrite the other system's **System Site Information**, nor will it be overwritten if changes are made to those systems.

-
- ❗ **IMPORTANT:** Although HP SIM currently does not require you to complete both **System Site Information** and **Customer Contact** sections, the Remote Support Pack requires both sections are filled out, especially the fields designated by *.
-

Example of setting system properties for multiple systems

This tool enables you to edit system properties for multiple systems at one time. The **Set System Properties** page for multiple systems is similar to the **Edit System Properties** page for a single system, except that a checkbox appears next to each property. The checkboxes enable you to select the properties you want to configure when the tool executes. Only the selected properties are saved as a property for the target systems. If the value of the selected property is blank, that property is not set for the systems **All properties** are optional.

NOTE: This tool can be used for a single system. However, some of the properties that are available from the **System Page** are not available when selecting this option. For example, the serial number is not available here, whereas it is available from the **System Page**.

NOTE: To complete this procedure, you must be authorized to use the **EDIT_SYSTEM_PROPERTIES** tool on the systems you want to update.

See the HP SIM online help for information on editing system properties.

13 Event management

Events are typically sent to the CMS from agents running on the managed systems. However, some events are generated directly from the CMS itself. Managed systems must be configured to send events to the CMS. After the CMS receives the event, if it passes the filters, any actions configured to happen upon its receipt are run, and the event is stored in the HP SIM database for later viewing. The event list page is the view for an event collection and lists of events that meet common criteria. From this page, you can clear, delete, and assign events, enter comments on the event, and view printable reports. To access the event list page, select an event collection from the **System and Event Collections** panel.

Monitoring [events](#) in HP SIM includes the following tasks:

- **Automatic Event Handling**
Enables you to manage automatic event handling tasks, create new automatic event handling tasks, and configure e-mail and modem settings.
- **Clearing Events**
Enables you to clear events. Select **Options**→**Events**→**Clear Events**. Select the target events to clear and click **Clear**.
Cleared events remain in the HP SIM database, but no longer contribute to the status icon reported in the System Status panel.
- **Deleting Events**
Enables you to delete events from the database.
Select **Options**→**Events**→**Delete Events**. Select the events to delete and click **Delete**. The events are deleted from the database. This tool can be scheduled to run on a regular basis. For more information, see [“Default system tasks”](#) (page 210).

NOTE: You can also delete events from the event view page.

Event management configuration

The following menu options are used to configure event management:

- **Event Filter Settings**
Enables you to filter SNMP [traps](#) you receive from discovered [systems](#). The default setting is to accept all registered [SNMP traps](#) from all discovered systems. You can specify the severity of the traps you want to see and use the IP address ranges to create a subset of systems whose traps you can receive or ignore. For example, you can use event filtering to ignore informational traps. This feature is available to users with administrative rights.
To access **Event Filter Settings**, select **Options**→**Events**→**Event Filter Settings**.
- **SNMP Trap Settings**
Enables you to tailor trap messages to your specific network needs. Trap messages can be cryptic, poorly written, and incomprehensible. You can modify the [Management Information Base](#) (MIB) information in the database representation. You can also modify a `.cfg` file of the MIB. HP recommends that you never modify an actual MIB. To access SNMP trap settings, select **Options**→**Events**→**SNMP Trap Settings**.
SNMP trap settings are available to users with administrative rights and are used to view or edit trap details for a registered MIB.

- **Status Change Event Settings**

Enables you to control if a status change event is generated when health status changes. To access, select **Options→Events→Status Change Event Settings**.

- **Subscribing to WBEM Events**

Enables you to subscribe to WBEM events. Select **Options→Events→Subscribe to WBEM Events**.

- **Unsubscribing to WBEM Events**

Enables you to unsubscribe to WBEM events. Select **Options→Events→Unsubscribe to WBEM Events**.

Example - Creating a paging task based on e-mail notification

You can set up a notification task to forward an e-mail to a cell phone (for example, [Short Message Service \(SMS\)](#)) or other paging interface applications, whenever the CMS receives a Critical, Major, or Minor event.

❗ **IMPORTANT:** When using time filters, you can use on-call style e-mails or pages. If you want one person to be notified during business hours and another at night, create two different tasks and set the time filter appropriately.

NOTE: This same type of task configuration can be applied to a Paging Task to use a modem in the HP SIM server to page through a cell phone or alphanumeric pager.

NOTE: Paging is only supported on a CMS running Windows.

Procedure 10 Setting notification task to forward e-mail to cell phone

1. Select **Options→Events→Automatic Event Handling→New Task**. The **Automatic Event Handling - New Task** page appears.
2. In the **Task name** field, enter a name for the task, such as **Important Events for e-mail-Pager Task**.
3. Click **Next**. The **Select event collection** page appears.
4. Select **use event attributes that I will specify**.
5. Click **Next**. From the second selection box (comparison selection) on the **Select Events** page, click the dropdown list, and then select **is**.
6. From the third selection box (value selection), the available values for a given criteria or comparison combination are given. Select **Informational**.
7. Click **Add**.
8. From the third selection box (value selection), the available values for a given criteria or comparison combination are given. Select **Critical**.
9. Repeat steps 5-8, and in the third selection box, select **Major** and then **Minor**.
10. Click **Next**. The **Select system collection** page appears.
11. Select **Use system attributes that I will specify**.
12. Click **Next**. The **Select systems** page appears.
 - a. In the first selection box (criteria selection), select **system name**.
 - b. In the second selection box (comparison selection), select **is**.
 - c. In the third selection box (value selection), select **(any)**.
 - d. Click **Next**. The **Select actions** page appears.

13. Select **Send e-mail**.
 - a. In the **To** address field, enter the e-mail address to which you want the notification sent (multiple addresses can be added so that a group is notified). A **CC** address can also be added so that a manager or supervisor is also notified.
 - b. In the **Subject** field, enter your subject. For example, **HP Systems Insight Manager Events**.
 - c. In the **Message Format** section, change the option to **Pager/SMS**. This option sends a condensed e-mail format that is similar to a paging task in HP SIM, which is the ideal way to send alerts to a cell phone type of hardware (or when Telephony Application Programming Interface (TAPI) is not available and an e-mail-to-paging provider is being used).
14. Click **Next**. The **Select time filter** section appears.
15. Select **Use time filter** and select **Nights and Weekends**, unless you want to receive the e-mail 24 hours per day. If so, clear **Use time filter**.
16. Click **Next**. The **Review summary** page appears.
17. Click **Finish** to create the new task.

Examples of e-mail pages

Automatic Event Handling enables you to send a system's home page URL in an e-mail address if that system has a home page. If the system does not have a home page, then Automatic Event Handling sends a URL that points to the HP SIM **System Page** of the system on the current CMS.

NOTE: The URL specified in an e-mail message appears only if the format is set to standard.

You can send the following e-mail pages from HP SIM:

- Standard
- Pager/SMS
- HTML

Example of a standard e-mail page

From: Doe, John
Sent: Wednesday, April 28, 2004 5:04 PM
To: Doe, Jane
Cc: Smith, Jim; Jones, Beth
Subject: System A: Storage System side panel is removed (Ver. 3):
Standard E-mail format

Event Name: Storage System side panel is removed (Ver. 3)
URL: https://systemname:2381
Event originator: System A
Event Severity: Major
Event received: 28-Apr-2004, 17:03:47

Event description: Storage System side panel is removed. The side panel status has been set to removed. The storage system's side panel is not in a properly installed state. This situation may result in improper cooling of the drives in the storage system due to air flow changes caused by the missing side panel.

User Action: Replace the storage system side panel.

Status: sidePanelRemoved

Example of a Pager/SMS page

From: Doe, John
Sent: Wednesday, April 28, 2004 5:04 PM
To: Doe, Jane
Cc: Smith, Jim; Jones, Beth
Subject: System A: Storage System side panel is removed
(Ver. 3): Pager
SMS Format E-mail testing

System A, Storage System side panel is removed (Ver. 3),Status:
sidePanelRemoved

Example of an HTML page

From: Doe, John
Sent: Wednesday, April 28, 2004 5:04 PM
To: Doe, Jane
Cc: Smith, Jim; Jones, Beth
Subject: qaunit1: Storage System side panel is removed (Ver. 3): HTML
Format E-mail testing

Event Identification and Details	
Event Severity	Major
Cleared Status	Not cleared
Event Source	qaunit1
Associated System	qaunit1
Associated System Status	Minor
Event Time	28-Apr-2004, 17:03:47 CDT
Description	Storage System: side panel is removed. The side panel status has been set to removed. The storage system's side panel is not in a properly installed state. This situation may result in improper cooling of the drives in the storage system due to air flow changes caused by the missing side panel. User Action: Replace the storage system side panel.
Assignee	May-HTML
Comments	

Trap Details	
Variable Description	Value
An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name.	QAUNIT1
The Trap Flags. This is a collection of flags used during trap delivery. Each bit has the following meaning: Bit 5-31: RESERVED: Always 0. Bit 2-4: Trap Condition 0= Not used (for backward compatibility) 1= Condition unknown or N/A 2= Condition ok 3= Condition degraded 4= Condition failed 5-7= reserved Bit 1: Client IP address type 0= static entry 1= DHCP entry Bit 0: Agent Type 0= Server 1= Client NOTE: bit 31 is the most significant bit, bit 0 is the least significant.	0
Drive Box Side Panel Status: This value will be one of the following: other(1) The agent does not recognize the status. You may need to upgrade your software. sidePanelInPlace(2) The side panel is properly installed on the storage system. sidePanelRemoved(3) The side panel is not properly installed on the storage system. noSidePanelStatus(4) This unit does not support side panel status monitoring.	sidePanelRemoved

Where *quanit1* is the system name.

Example - Creating a task to send an e-mail when a system reaches a critical state

The following instructions set up an automatic event handling task to be run when a discovered system goes to a [Critical status](#).

Procedure 11 Creating a task to send an e-mail when a system reaches a critical state

1. In the **Search** panel, click **Advanced Search**. The **Advanced Search** page appears.
2. Select **events** from the **Search for** dropdown list.
3. From the first selection box (**criteria** selection), select **severity** from the dropdown list.
4. From the second selection box (comparison selection), select **is** from the dropdown list.
5. In the third selection box (value selection), the available values for a given criteria or comparison combination are given. Select **Critical**.
6. (Optional) Click **View** to view the search results.
7. Click **Save As Collection** to save the event collection.
8. In the **Name** field, enter a name for the collection, such as **Critical Events**.
9. Under **Place in**, select to save the collection in **Events by Severity** to have it available to other users.
10. Click **OK** to save the collection, or click **Cancel** to cancel the save operation.
11. To configure HP SIM to send an e-mail, select **Options**→**Events**→**Automatic Event Handling**→**E-mail Settings**. The **E-mail Settings** page appears.
12. Specify the SMTP host in the **SMTP Host** box.
13. Specify the e-mail address that the management server uses when sending e-mail notifications in the **Sender's Email Address** box.
14. To authenticate your SMTP server, select the **Server Requires Authentication** checkbox.
15. Specify the account name in **Account name** box.
16. Specify the password in the **Password** box.
17. Click **OK** to save changes.
18. To configure status change events, select **Options**→**Events**→**Status Change Event Settings**. The **Status Change Event Settings** page appears.
19. Select **Enable creation of system status change events**. This option sends a system unreachable event whenever a system cannot be reached by a ping through the Hardware Status Polling task. Enabling this option creates a system reachable event whenever the system is reachable again.
20. Click **OK** to apply changes.
21. To create the task, select **Options**→**Events**→**Automatic Event Handling**→**New Task**. The **Automatic Event Handling - New Task** page appears.
22. On the **Step 1, Select name** page, enter a name for the task in the **Task name** box, such as **Send E-mail for Critical Status**.
23. Click **Next**. The **Step 2, Select event collection** page appears.
24. Select the **Critical Events** collection from the dropdown list.
25. Click **Next**. The **Select system collection** page appears. Do not select a system collection.
26. Click **Next**. The **Select action** page appears.
27. Select **Send e-mail**.
 - a. In the **To** field, enter the list of e-mail addresses that should receive the notification.
 - b. In the **CC** field, enter any e-mail address that should receive a copy of the e-mail, separating each with a comma.
 - c. In the **Subject** field, enter a note describing the subject of the e-mail.

- d. In the **Message Format** field, select from the following formats based on the encoding preference of the recipient:
 - **Standard**. This default message format sends a text e-mail message to the recipients.
 - **Pager/SMS**. An e-mail message formatted with the same information and format as a pager message is sent to the recipients.
 - **HTML**. An e-mail message that looks like the **HTML Event Details** page is sent to the recipients.
 - e. In the **Encoding** field, select from the following formats:
 - **Western European (ISO-8859-1)**
 - **Unicode (UTF-8)**
 - **Japanese (ISO-2022-JP)**
 - **Japanese (Shift_JIS)**
 - **Japanese (EUC-JP)**
 - **S-Chinese (GB18030)**
 - **T-Chinese (Big5)**
 - **Korean (EUC-KR)**
28. Click **Next**. The **Step 4, Select time filter** page appears.
 29. Select the **Use time filter** box if you want to use time filters, and then select an option from the dropdown list.
Click **Manage Filters** if you want to set user defined filters.
 30. Click **Next**. The **Step 5, Review summary** page appears. The **Task name**, the **selected event collection**, the **events**, **system criteria**, and **Action(s)** information appear.
 31. If you want to edit the e-mail selections, click **Edit e-mail Settings** to edit the SMTP settings.
 32. Click **Finish** to create the new task.

Example - Creating a task to delete all cleared events

The following example describes how to create a task to delete all cleared server events from the HP SIM database. This task is useful to include in your management portfolio because deleting cleared events on a regular basis empties the database of unnecessary entries and improves system performance.

The following task has the following segments:

- Creating an event collection that contains the events you want to delete
- Creating and scheduling the task to delete all cleared server events and run the task

Procedure 12 Creating a task to delete all cleared events

1. In the **Search** panel, click **Advanced Search**. The **Advanced Search** page appears.
2. Select **events** from the **Search for** dropdown list.
3. From the first selection box (**criteria** selection), select **cleared state** from the dropdown list.
4. From the second selection box (comparison selection), select **is** from the dropdown list.
5. In the third selection box (value selection), select **cleared**.
6. (Optional) Click **View** to view the search results.
7. Click **Save As Collection** to save the event collection.
8. In the **Name** field, enter a name for the collection, such as **Delete Cleared Server Events**.
9. Under **Place in**, select to save the collection in **Events by Severity** to have it available to other users.

10. Click **OK** to save the collection.
11. Then select systems from the **Search** dropdown list.
12. From the first selection box (criteria selection), select **system type** from the dropdown list.
13. From the second selection box (comparison selection), select **is** from the dropdown list.
14. In the third selection box (value selection), the available values for a given criteria or comparison combination are given. Select **server**.
15. (Optional) Click **View** to view the search results.
16. Click **Save As Collection** to save the system collection.
17. In the **Name** field, enter a name for the system collection, such as **Delete Cleared Server Events_system**.
18. To create and schedule the task, select **Options→Events→Delete Events**. The **Delete Events** page appears.
19. Select the *Delete Cleared Server Events* collection from the dropdown list
20. Click **Apply**.
21. Now click **Add system filter** to add the system collection.
22. Select the system collection created in step 17, select "**Delete Cleared Server Events_system**" **itself**.
23. Click **Apply**.
24. Click **Schedule**.
25. In the **Task name** box, give the task a name, such as **Delete Cleared Server Events** task.
26. In the **Refine schedule** section, select the scheduling option that you prefer.
In this example, if you select **When new systems or events are added to the collection**, then HP SIM automatically deletes server events whenever they become cleared.
27. Click **Done**. The task is scheduled and the **All Scheduled Tasks** page appears.
To run this task at any time, select **Tasks & Logs→View All Scheduled Tasks** . Then select **Delete Cleared Server Events** from the table and click **Run Now**.

14 Reporting in HP SIM

Standard reports

Standard reports are shipped with HP SIM. The reports are based on common user scenarios and do not need any additional configuration or enablement. These reports are installed, configured, and available for use as soon as HP SIM is installed and configured. Standard reports are tied to existing systems collections in HP SIM, for instance, **All Systems** or **All Servers**. Report results appear based on logged in user authorization of systems.

Standard reports are available by navigating to the **Manage Reports** page .

New Reports

A report configuration is a customer-defined set of preferences that pulls specified criteria from the database tables and places it in a report in the specified format. The report configurations can be saved and used to run a report at a later date with live data.

You must have administrative or [operator rights](#) to create, save, edit, copy, or delete report configurations. [Users](#) with [user rights](#) can run the authorized report configurations only.

If User 1 with administrative rights generates a report and a private collection, then User 2 with administrative rights is allowed to generate a report using the report configuration and private collection that User 1 created. User 2 is allowed to edit, save, and delete the report configuration but cannot delete the private collection created by User 1.

The create new report wizard helps you to create a new report and add it to HP SIM reports. This option is only available for HP SIM.

You can save the report configuration for future use or generate a one-time report.

Select **Reports**→**New Report...**, the **Step 1: Select Target Systems** page appears. Verify target systems and click **Next**. The **Step 2: Specify Parameters** page appears. Provide a name for the report, and check the required items under **Select items** to show in the report and save the report.

Managing reports

The Manage Reports feature provides you with the following options:

- **Run Report**

A generated report provides you with the following information:

- Report name
- Associated system collection

NOTE: The Associated system collection information does not appear if there is no collection selected to run the report.

- Report run date and time

Format for generated report:

- **HTML (Recommended for viewing)**
Enables viewing an existing report in HTML format.
- **XML**
Enables viewing an existing report in XML format.
- **CSV**
Enables viewing an existing report in CSV format.
- **Copy**
HP SIM enables you to copy report configurations from an existing report configuration. You can edit the newly copied configurations to create a new report.

NOTE: You must be signed in to HP SIM with [administrative rights](#) or [operator rights](#) to copy report configurations. If you are not signed in with administrative or operator rights, the copy option is not available.

- **New**
Enables you to create a new report and add it to HP SIM reports. This option is only available for HP SIM.
You can save the report configuration for future use or generate a one-time report.
- **Edit**
HP SIM enables you to edit existing report configurations. You can save these updated report configurations over the existing report configuration, or you can save it as a new report configuration.

NOTE: You must have [administrative rights](#) or [operator rights](#) to create, save, edit, copy, or delete report configurations. Users with [user rights](#) cannot edit the report configurations.

- **Delete**
You can permanently delete a report configuration from the **Manage Reports** page.
- **Showing SQL Queries.**
Enables viewing SQL queries.
Select **Reports→Manage Reports....** The **Manage Reports** page appears. Select the report for which you want to view the SQL details, select **Run Report**, and then on the report itself, click **Show SQL queries**.

Snapshot Comparison

Snapshot comparisons enable you to compare up to four systems (with the same operating system) to each other or to compare a single system to itself and observe changes over time.

To view a snapshot comparison, select **Reports→Snapshot Comparison....** The **Snapshot Comparison** page appears. Select target systems, and then click **Next**.

Enhanced Reports

Enhanced reports contain the **Reports by Product** table that displays the products registered with HP SIM along with the available reports. There are 18 predefined reports under HP SIM enhanced reports.

The reporting engine main page contains the **Reports by Product** table that displays the products registered with HP SIM along with the available reports.

The **Reports by Product** table displays reports for HP SIM by default. Only products that have been registered with HP SIM have [Predefined](#) reports displayed.

Table 6 Reports by Product columns

Name	Description
Product/Report Name	Displays the name of the products along with the total number of reports in parenthesis registered with HP SIM for reports. When the product item is expanded by clicking the expand icon, the available reports are displayed under the product section along with report details Description , Target Systems and Report Type .
Report Type	Displays the type of report such as; Table , Bar , Pie , Bar-Pie , or Line .
Target Systems	Displays the target selection in which the report is executed.
Description	Displays a short description of the report.

Table 7 Reports by Product buttons

Name	Description
New	Creates a new report.
Edit	Edits a selected report. Only enabled for user created/defined reports under HP SIM. Remains disabled for Predefined reports.
Run Report	Executes a report.
Email Report	Enables users to email a report.
Delete	Deletes a selected report. Only user created/defined reports can be deleted.

Predefined reports

Predefined Reports are shipped with HP SIM. The reports are based on common user scenarios. **Predefined Reports** are tied to existing system collections in HP SIM, for instance, "**All Systems**" or "**All Servers**". Report results appear based on logged in user authorization of systems.

Select **Reports**→**Enhanced Reports**. The **Enhanced Reports, Reports by Product** page appears.

Run Enhanced reports

Running reports executes an available report in the reporting engine. The generated report is displayed in a new page when **Run Report** is clicked.

A generated report provides you with the report name, associated system collection, and report run date and time in the following formats. You select the format before you run the report.

- HTML (Recommended for viewing)
- CSV
- PDF

Select **Reports**→**Enhanced Reports**. The **Enhanced Reports** page appears. Select the report that you want to run. Click **Run Report**.

New Enhanced reports

A report configuration is a customer-defined set of preferences that pulls specified criteria from the database tables and places it in a report in the specified format. The report configurations can be saved and used to run a report at a later date with live data.

An additional create new report option is to select the type of report to use. You can select the following options in any combination.

- Include Chart
- Include Table

The report type graph supports three sub types.

- Bar
- Pie
- Line (Trend)

The **Include Chart** section dynamically changes to display the selection items that are required to create the corresponding report. Depending on the type of chart selected, additional details are presented as follows.

- **Graph Title**
The graph title is available for all chart types.
- **Footer**
The footer is available for all chart types.
- **X-axis**
The X-axis is available for a bar or line chart.
- **Y-axis**
The Y-axis is available for a bar or line chart.

The **Include Table** option allows the selection of the column fields and order to be displayed in the table of the generated report.

You can save the report configuration for future use or generate a one-time report.

Editing Enhanced reports

Only custom reports can be edited.

The details from the opened report are pre-populated in the text fields. The **Edit** button is only enabled for custom reports under HP SIM

E-mailing reports

E-mailing reports enables you to schedule a report to be run at a specified time and sent through e-mail. You can schedule a report to be run periodically or once. Select from the following options to run the report.

- Select **Run when the central management server is started** if you want the report to run when the central management server is started.
- Select **Run now** if you want to run the report immediately.
- Select **Disable this task** if you want to disable the report at any time.

Deleting reports

User-created reports located in the **Reports by Product** section can be deleted. Before the report is deleted, a popup message displays asking if you are sure you want to delete the selected report.

If you click **OK**, the report is deleted and the product and report page is refreshed to show the correct status of the reports.

15 HP SIM tools

Target selection

Targets are systems that a tool acts upon. Targets can be single systems, collections, or groups of systems that are chosen just for the task at hand. You can select the targets either before or after selecting the tool. You can verify and modify the selection using the task wizard.

After the targets are verified, they appear in the title area of the tool.

NOTE: Some tools cannot work on multiple systems. In this case, a warning is displayed that states you can select only an individual system.

See the Systems Insight Manager online help for more information on the task wizard.

Scheduling tools

The following options are available when scheduling tools to run:

- **Periodically**

Select from intervals of minutes, hours, days, weeks, or months. With periodic scheduling, you can configure the task to run until a certain date and time or to execute only a set number of times. Periodic scheduling allows time filters to be applied. These filters specify the hours of the day when a scheduled task can operate.

NOTE: If you want to schedule a task to run once a month on the 31st of the month and the month has only 30 days, the task will run on the 1st day of the following month.

- **Once**

Specify the date and time the task is to run.

- **When new systems or events are added to the collection**

This option is only available if you select a **Collection of Systems or Events** as your target. The task runs only when new systems or events meet the collection criteria. You can also apply a time filter to this type of scheduling.

- **When systems or events are removed from the collection**

This option is almost identical to the previous option, except that the task runs only when systems contained in the **Collection of Systems or Events** no longer meet the collection criteria. A time filter can be applied to this type of scheduling.

- **Not Scheduled**

This option specifies that the task runs only when manually executed by a user with appropriate privileges. This task never runs automatically. Tasks can be manually run from the **All Scheduled Tasks** page or the CLI.

Managing with tasks

HP SIM enables you to manage [systems](#) and [events](#) by scheduling and executing tasks. Tasks are actions performed using an HP SIM [tool](#). Task instances are an executed single instance of a [task](#).

Users can:

- Create a variation of a task
- Schedule a task
- Modify a task

- Delete a task
- Stop an executing task
- Track task status

Task information is available by selecting one of the following:

- **Tasks & Logs**→**View All Scheduled Tasks**
- **Tasks & Logs**→**View Task Results**

HP SIM provides system-delivered (default) tasks. These tasks can be disabled or have their schedules modified but they cannot be removed or reassigned to another user. HP SIM requires these tasks (for example, Data Collection) to provide a complete picture of the systems being monitored.

Viewing results

After a task runs, you can view the task results by selecting **Tasks & Logs**→**View Task Results**. The **Task Results** page appears and includes a table displaying all tasks that are complete or currently running. The table includes information on the launching task, the tool used, status of the task, who ran the task, and the start and end time of the task.

Example - Device ping

Use the Ping tool to ping an individual system or multiple systems. To ping systems, select **Diagnose**→**Ping**. The **Ping** window appears. Select the target systems and click **Run Now** to run the task.

If a system does not resolve to an IP address, the request cannot be performed. For systems with multiple IP addresses, the result of each IP address occupies one row in the result page. The status on the upper-right corner is: *Pinging selected systems*. After all the systems on the list are pinged, the status is: *Ping completed* with a time stamp of the completion time.

The ping results appear in a separate window. You might receive the following replies:

- *Replied*. The request has been executed successfully, and the pinged system has responded.
- *Request timed out*. The request has been executed, but the pinged system failed to respond.
- *System does not have an IP address and cannot be pinged*. There is no IP address associated with the system. Unable to perform ping.

If the ping is successful, there is no retry. You can retry only when the ping fails. The ping results have no effect on the system status on the **Task Results** or system view pages.

Part IV HP SIM advanced features

16 Collections in HP SIM

Collections in HP SIM

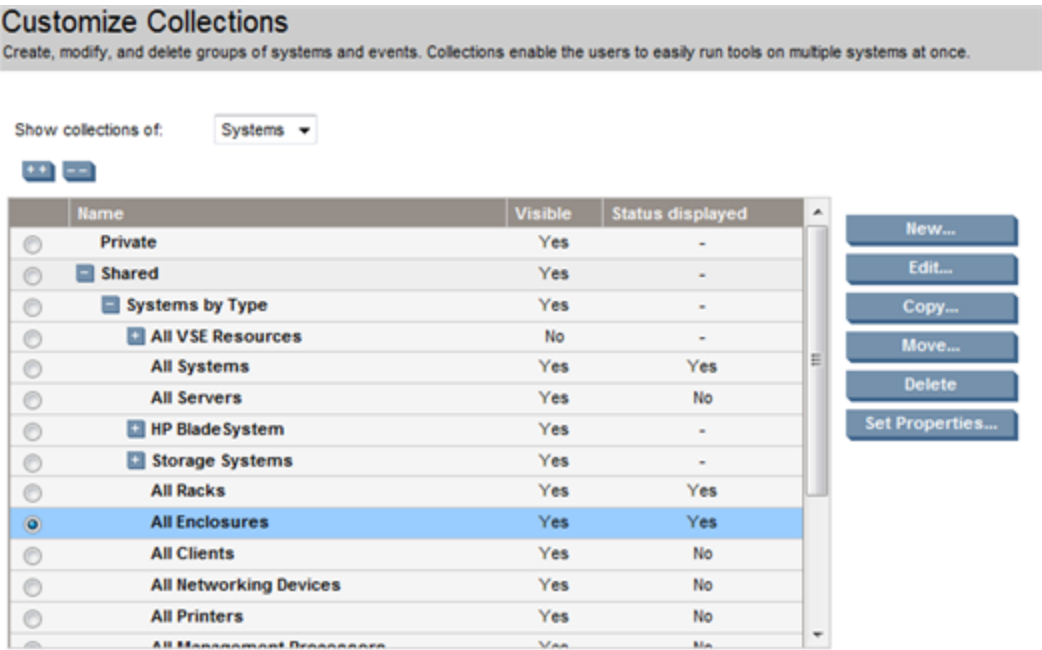
Systems and events are grouped into collections based on information from the HP SIM database. After a collection is defined, you can display the results or associate the collection with a task. You can also save an edited or unedited collection as a collection with another name.

You can use collections to organize large numbers of systems into smaller, more meaningful groupings. For example, your organization might have five system administrators who are responsible for 100 different systems in 6 different buildings. You can create a collection for each administrator that includes only his or her systems, or you can create a collection for each building that includes only the systems located in that building. You must have administrative rights to customize shared collections.

NOTE: Use English text for naming collections. If you do not use English text, you might see named collections generated by HP SIM. For example, *collection-**<number>***

You can create a collection several ways:

- Create a collection from the **Customize Collections** page.
Click the **Customize** link on the **System and Event Collections** panel. The **Customize Collections** page appears. Select **Events** or **Systems** and click **New**. The **New Collection** section is displayed.
Customize Collections page



NOTE: Both systems and event collections can be created.

- Create a collection from the system view page.
Click **Save As Collection** at the bottom of any system view page. This command enables you to save the currently selected systems (or collections) as a new collection.
Saving from the table view page

Financial Servers Maximize ?

System(s) Events Quick Launch...

View as: table

☐ Select "Financial Servers" itself

Summary: 0 Critical 0 Major 0 Minor 4 Normal 0 Disabled 5 Unknown Total 9

	HS	MP	SW	VPM	PF	ES	System Name	System Type	System Address	Product Name	OS Name
☐	?	?	?	?	?	?	UTS01-12080X	Server		ProLiant DL360 G4p	
☐	?	?	?	?	?	?	UTS02-12080X in End: Marketing_28U12080X18.00	Server		ProLiant BL460c G1	
☒	?	?	?	?	?	?	UTS02-12080X in End: Marketing_28U12080X18.00	Server		ProLiant BL460c G1	
☐	?	?	?	?	?	?	UTS02-12080X in End: Marketing_28U12080X18.00	Server		ProLiant BL460c G1	
☐	?	?	?	?	?	?	UTS02-12080X in End: undefined_	Server		ProLiant BL460c G1	
☐	?	?	?	?	?	?	UTS02-12080X	Server		ProLiant DL360 G5	
☐	?	?	?	?	?	?	UTS02-12080X	Server		ProLiant DL360 G5	
☐	?	?	?	?	?	?	UTS02-12080X	Server		ProLiant DL360 G5	
☐	?	?	?	?	?	?	UTS02-12080X	Server		ProLiant BL460c G1	

Save As Collection... Delete Print

- Run a [system search](#) and save the search criteria as the attributes defining a collection. Saving a collection from the Advanced Search page

Advanced Search Maximize ?

Search for matches based on selected criteria

Search for: systems

where: operating system

name is Windows Server (R) 2008 Enterprise, x64 Enterprise Edition Service Pack 1 (Service Pack 1, Build 6001 Multiprocessor Free)

and version is 6.0

and system type is Server

Delete Delete << Add View Save As Collection...

For more information on saving collections, see the Systems Insight Manager online help.

Types of collections

- By member

When you create a collection, you can select exactly which specific systems or collections you want to include. From the, **Customize Collections** page, click **New**. The **New Collection** section appears. Select **Choose members individually**.

NOTE: When you create event collections, you cannot select individual events. However, you can select event collections, which enables you to create a convenient hierarchy.

- By attribute

When you create a collection, you can describe the contents of the collection by the attributes of its members. Collections defined by attributes are dynamic because each time they are invoked, the contents are determined again.

You can use many system attributes for creating collections, for example, system name (full or partial), operating system, or system type. For event collections, some of the attributes you can select are [cleared status](#), type, severity, and time. You can combine multiple attributes to create the exact group of systems or events that you need.

To create collections by attribute, click **Save As Collection** from the **Advanced Search** page or click **New** from the **Customize Collections** page. Then, in the **New Collection** section, select **Choose members by attributes**. Select the attributes and click **Save As Collection**

Because collections by attribute use a database query, collections that are complex take more system resources every time they are accessed. Keeping collections simple minimizes performance impact.

- Combination collections

Combination collections enable you to bind together a system collection and an event collection and to reuse and recombine system and event collections that you have created.

NOTE: There are two kinds of combination collections. If you are creating a system collection, then the combination collection returns a system list. If you are creating an event collection, then the combination collection returns an event list. For example, the two collections **All Servers** and **All Login and Logout Events** could be combined in two ways. One way yields all servers that have login and logout events. The other way yields all login and logout events that occurred on servers.

Creating a System Collection

To quickly see all system management processors, log in to HP SIM. In the **System and Event Collections** panel, scroll down to and select **All Management Processors**.

The **All Management Processors** page appears.

To create a custom group of all iLO devices (or by iLO version), create a system collection.

1. In the **System and Event Collections** panel, click **Customize**. The **Customize Collections** page appears.
2. In the **Show collections of** dropdown list, select **Systems**.
All available system or cluster collections appear.
3. Click **New**. The **New Collection** section appears.
4. Select **Choose members by attributes**.
5. In the **Search for** dropdown list, select **systems**.
6. In the **Where** dropdown list, select system sub type, and select is from the inclusion/exclusion dropdown list.
7. Select an Integrated Lights-Out choice from the system sub type dropdown list at the right.
8. Click one of the following:
 - View — runs the search and display results immediately.
 - Save as Collection — saves the collection.
 - Cancel — closes the **New Collection** section without saving any changes.

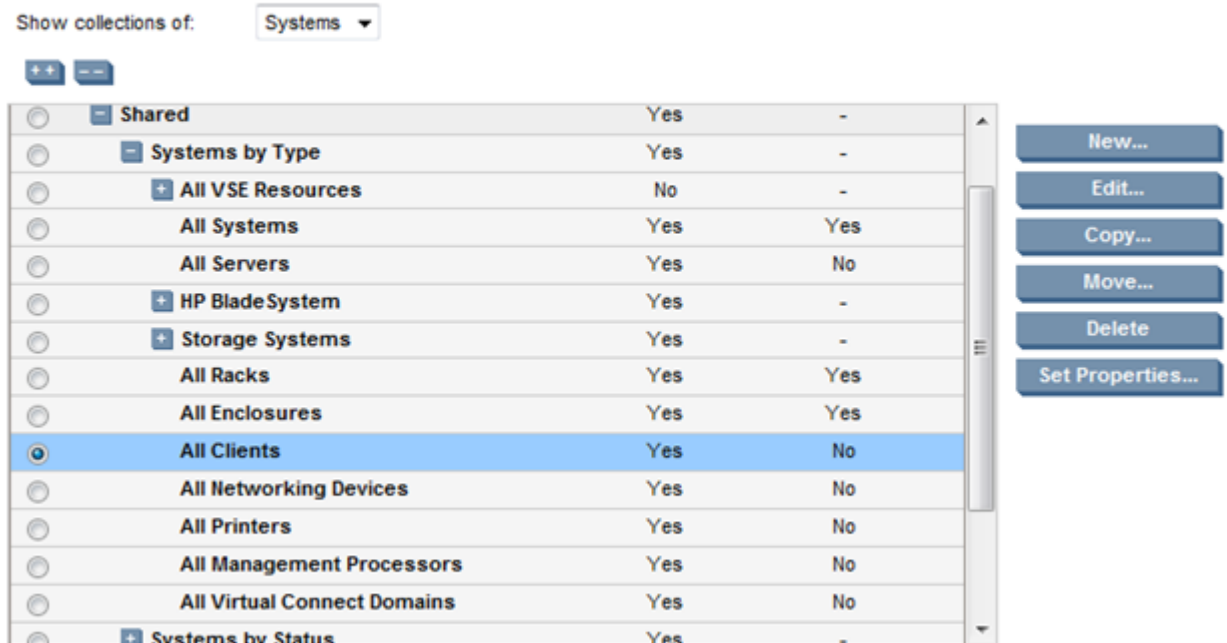
Other customization features

The **Customize Collections** page enables you to create and organize your collections in a way that works for you.

Customize Collections page

Customize Collections

Create, modify, and delete groups of systems and events. Collections enable the users to easily run tools on multiple systems at once.



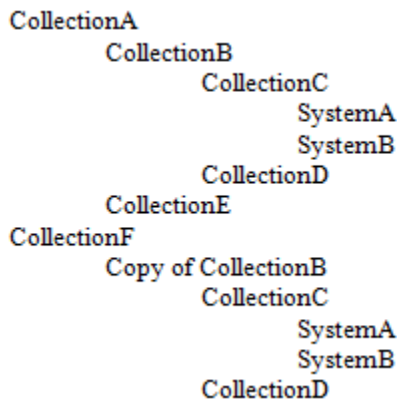
On the **Customize Collections** page, some collections show their contents and others do not. For example, in the above image, **All Systems**, **HP BladeSystems**, and **Storage Systems** are not collections by member because the expansion icon (+) is located beside the collection name, and when you click the icon, the contents of the collection are displayed.

Because collections by attribute are dynamic, determining their content and displaying it in this interface would be very time consuming. Therefore, their content is not displayed and you cannot set properties on members of these collections. Setting properties on systems that might not be part of the collection in the future would be of very limited value.

- **Edit**
Any collection can be edited. However, collections cannot change type. For example, you can change the criteria for a collection that is defined by attribute, but you cannot change the collection type so the collection is a collection by member or a combination collection.
- **Copy**
Copy enables you to copy a collection from one place in the collection hierarchy to another. It is important to note that what is copied is independent of the original collection; any collections that are within the copied collection are themselves copied by reference.
For example, consider the following hierarchy (contents of the collections not relevant to the example are not shown):

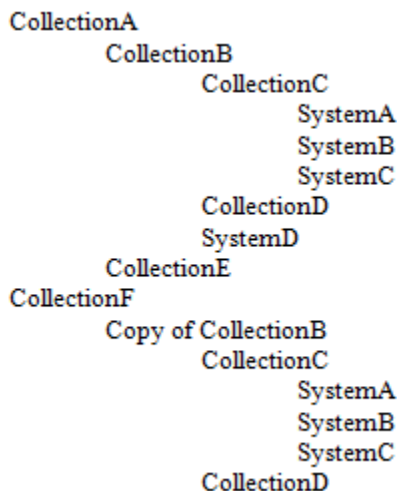
```
CollectionA
  CollectionB
    CollectionC
      SystemA
      SystemB
    CollectionD
  CollectionE
CollectionF
```

If CollectionB is copied to CollectionF, the hierarchy would look like the following:



The new instance of CollectionB receives a new name, but its contents are copied directly. The contents, CollectionC and CollectionD, are copied by reference. Both CollectionB and Copy of CollectionB refer to the exact same instances of CollectionC and CollectionD.

Later, if SystemC is added to CollectionC, and SystemD is added to the original CollectionB, the result would be that SystemC appears in both places, and SystemD appears only in one place, as follows:



There are two instances of SystemC in the view of the hierarchy because CollectionC is the same throughout the application. Any place that CollectionC is referenced, it will always contain the same systems. However, SystemD appears only under CollectionB. CollectionB and Copy of CollectionB are distinct and independent collections.

- Move

Move enables you to easily move a collection exactly where you want it in the hierarchy.

NOTE: Collections can be moved from **Private** to **Shared**, but not from **Shared** to **Private**.

- Delete

Most collections can be deleted. However, there are some restrictions.

- Collections cannot be deleted if they are not empty.
- Collections cannot be deleted if they are in use. That is, if the collection is the target for a scheduled task, if it is used for the **System Status** panel, or if it is used in some other collection, then it cannot be deleted.

- The **All Systems** and **All Events** collections cannot be deleted.
- After a collection is deleted, it cannot be recovered.
- Set Properties

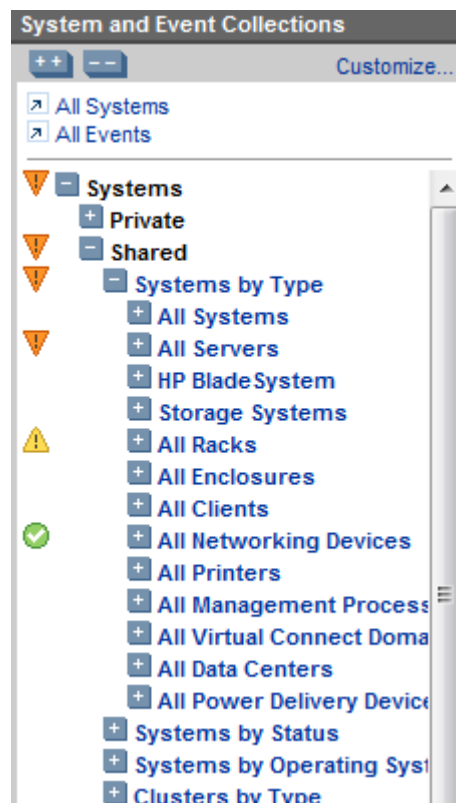
Collections have properties, and these properties define the way collections behave in the **System and Event Collections** panel and elsewhere in HP SIM.

 - Visible property

It might be the case that there are system or event collections, that are either shipped with HP SIM or are user-defined, that you do not use, but at the same time, do not want to delete. If you do not use these collections, but you do not want to delete them, you can remove them from the user interface by using the **Visible** setting in the collection properties. When you select **No, do not show collection and its members in the user interface** for a collection, that collection no longer appears in the **System and Event Collections** panel, in the Task Wizard, or any place in the user interface (except the customization panel itself) where collections are shown.

Making collections invisible can make the **System and Event Collections** panel less cluttered, but note that once you make collections invisible, they are excluded everywhere in HP SIM including being removed from tasks. For example, if a task is scheduled to run with a certain collection, and that collection is made not visible, then the task will not run on that collection. You can change the visibility setting at any time.
 - Status Displayed property

You can set the **Status Displayed** property to enable you to easily view the aggregate status of a particular collection in the **System and Event Collections** panel. You can set this property only on individual systems or on collections by attribute, for example, the lowest displaying collection aggregate status.



level of the hierarchy (the leaves of the tree).

In the **System and Event Collections** panel, where the status is displayed, the status will "bubble up" to the higher levels of the hierarchy (the root of the tree) so that the most urgent statuses are always visible at any level.

Statuses are merged so that the most significant is always displayed.

NOTE: Statuses at the top of the following list take priority over those at the bottom.

- Critical
 - Major
 - Minor
 - Warning
 - Normal
 - Disabled
 - Unknown
 - Informational
 - Default View property
- When you select a collection in the **System and Event Collections** panel, the contents of that collection are displayed in the workspace. By default, different types of collections are displayed in different ways. Collections by attribute and combination collections default to a table view, but they can also be displayed as icons or a tree. Collections by members default to a tree view, but they can also be displayed as icons or a table. Special types of system collections default to picture views or special consoles. You can change the default view using this property.

17 HP SIM custom tools

General concepts

Custom tools are tools that can be created by the user to run on the CMS or on target systems. For example:

- **Remote tool**

A tool that runs on selected target systems. It might copy files to the target systems or run specific X-Window applications on the target systems. You can schedule this tool.

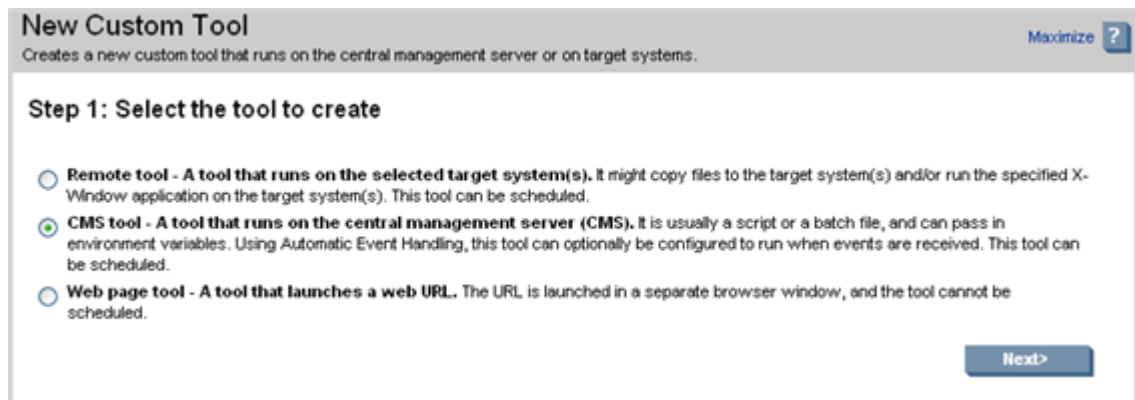
- **CMS tool**

A tool that runs on the CMS. It is usually a script or batch file and can pass in environment variables. Using Automatic Event Handling, you can configure this tool to run when events are received. You can schedule this tool.

- **Web page tool**

A tool that launches a web URL. The URL is launched in a separate browser window on the CMS. You cannot schedule this tool.

To add custom tools, you can either use the **Tools→Custom Tools→New Custom Tool** menu in the GUI, or edit the tool definition files (tdefs) in a text editor and register them with the CLI `mxtool`. Both procedures are explained in this chapter.



Tool types

As delivered, HP SIM provides an administrator with unified management control of any number of servers and storage devices from a single console in the data center or in a remote location. When customized with specialized tools or Insight Essentials Value Added Software plug-ins, HP SIM becomes a comprehensive, easy-to-use platform for controlling Microsoft Windows, Linux, or HP-UX enterprise environments.

A key method of administering multiple systems is through scripting. HP SIM features a modular architecture that uses [tool definition files](#) (TDEFs) written in the XML data file format. A TDEF contains the definitions of one or more tools used by HP SIM and define how a tool launches and executes. A tool can be a script or an executable file. Creating custom tools enables you to extend the use of HP SIM to your specific business environment.

Table 8 Tool types

Name	Description
Single-system-aware command tool OR Remote Tool in the GUI	An SSA tool executes on a selected target and is only aware of the target system environment. In executing an SSA tool, the HP SIM Distributed Task Facility (DTF) of the

Table 8 Tool types (continued)

Name	Description
	CMS uses SSH to send one or more files to the target system, which then executes the tool. An example of an SSA tool would be a tool that wraps a common Unix command such as ls , cat , or cp .
Multiple-system-aware command tool	An MSA tool executes typically on the CMS and can work with multiple target systems. When launched, the MSA process is created once and then passed to all targets on the list. An XWindows tool is an example of an MSA tool.
Web launch tool or Web page tool in the GUI	A WLA tool typically launches in a separate browser (by default) or in the same frame as HP SIM and is specified by a universal resource locator (URL). Web-launch applications that do not share HP SIM certificates should be executed in a separate frame.
Application launch tool or CMS Tool in the GUI	An application launch tool is a batch file, script, or executable that runs on the CMS and can reference environment variables specified by the tool to access device or event information. An example of an application launch tool would be one that performs a task that is tied to the contents of an Exchange Servers list which returns three devices (A, B, and C). The tool will run three times (in the context of A, B, and C).

Environment variables for custom tools

NOTE: If your user-defined variables have the same names as the HP SIM environment variables, the HP SIM environment variables override the user-defined variables.

DOS environment variables are supported in custom tool parameters and work as parameters on the **New Custom Tool** page or the **Manage Custom Tools** page. Unless you use DOS environment variables in a batch or script file, you must surround them with double percent (%) signs. For example, to pass in the **NOTICELABEL** environment variable as a parameter on the parameter line, enter **%%NOTICELABEL%%**. If you use DOS environment variables in a batch file or script file, use only a single percent (%) sign before and after the environment variable name.

NOTICELABEL. Type of notice. A small string that contains discovered system, other HP SIM server-level notices, or the type of trap that caused the notice.

NOTICESTATE. An internal value used by HP SIM, indicating whether the notice is cleared.

NOTICEPLAINTEXT. A text description of the notice that contains details about the notice (In Progress, Cleared, or Not Cleared).

NOTICERAWDATA. The raw data from the notice is passed as a string. This is a small pipe (|) delimited set of variables and might be useful for some simple parsing rules.

NOTICESEVERITYSTR. A verbose description of the notice severity, which can be Critical, Informational, Major, Minor, Unknown, Warning, or Normal.

NOTICESEVERITY. The integer value of the **NOTICESEVERITYSTR** which can be one of the following:

- 0, Unknown
- 1, Normal
- 2, Warning
- 3, Minor
- 4, Major

- 5, Critical
- 100, Informational

NOTICEQUERYNAME. The collection name based on how the notice was generated. This value can say one of the following:

- This system or event meets the following search criteria: +QueryName;
- This system or event now meets the following search criteria: +QueryName;
- This system or event no longer meets the following search criteria: +QueryName;

DEVICENAME. The name of the [system](#) that caused the notice.

DEVICEIPADDRESSCOUNT. The number of IP addresses that are mapped to this system.

DEVICEIPADDRESS%d. Based on the count, %d is an integer that shows the actual IP address. For example:

```
IF, DEVICEIPADDRESSCOUNT = 2
Then, DEVICEIPADDRESS0 = 111.111.111.111
DEVICEIPADDRESS1 = 222.222.222.222
```

DEVICEMACADDRESSCOUNT. The number of MAC addresses collected for the system. Before this information is available, you must run a Data Collection task.

DEVICEMACADDRESS%d. Based on the MAC address count, %d is an integer that references the actual MAC address environment variable. For example:

```
IF, DEVICEMACADDRESSCOUNT = 2
Then, DEVICEMACADDRESS0=00:80:5F:7F:B0:81
DEVICEMACADDRESS1=00:80:C7:29:EF:B6
```

GENERICTRAPID. The SNMP Generic Trap ID of the trap received, if this is an event-based list and originated from an [SNMP trap](#).

SPECIFICTRAPID. The SNMP Specific Trap ID of the trap received, if this is an event-based list and originated from an SNMP trap.

Path. The Path environment variable value from the context where the service is running

SystemRoot. The SystemRoot environment variable value, from the context where the service is running.

Windir. The Windir environment variable value, from the context where the service is running.

COMPUTERNAME. The COMPUTERNAME environment variable value, where the context in which the service is running.

MPIP. The IP address of the associated management processor.

MPNAME. The name of the associated management processor.

RELATEDDEVICECOUNT. The number of associated systems.

RELATEDDEVICENAME%d. The name of the associated system, where %d is the iteration number. For example:

```
IF, RELATEDDEVICECOUNT = 2
Then, RELATEDDEVICENAME0=DeviceName0
RELATEDDEVICENAME1=DeviceName1
```

RELATEDDEVICEIP%d. The IP address of the associated system, where %d is the iteration number. For example:

```
IF, RELATEDDEVICECOUNT = 2
Then, RELATEDDEVICEIP0=111.111.111.111
RELATEDDEVICEIP1=222.222.222.222
```

RELATIONSHIP%d. The relationship string with the associated system, and %d is the iteration number. For example:

```
IF, RELATEDDEVICECOUNT = 2
Then, RELATIONSHIP0=ServerToEnclosure
RELATIONSHIP1=VMGuestToVMHost
```

Launching applications using custom tools

Use custom tools in HP SIM to combine RIBCL, CPQLOCFG, and system collection to manage Group Administration of iLO systems. Custom tools are executed on the CMS, and on target systems. You can create a remote tool that runs on selected targeted systems, and even schedule its execution. For more information about custom tools, see the HP SIM help.

Custom tool menu placement

To place custom tools in the following menu locations, use a string in the form *base/submenu/subsubmenu*.

Menu level	Example
<i>top-level-menu</i>	Tools
<i>top-level-menu/first-level-cascade</i>	Tools Custom Tools
<i>top-level-menu/first-level-cascade/second-level-cascade</i>	Tools Custom Tools <i>My Tools</i>

For example, place a tool under **Tools→Custom Tools**, place an entry in the **Menu placement** field such as **Tools | CustomTools**.

By default, if the **Menu placement** field is left blank, the tools are placed in **Tools→Custom Tools**.

Custom tool URL format

The URL strings for web-aware tools and command line tools must be provided as absolute URLs beginning with `http://` or `https://`. For example,

```
https://%n:1188/kcweb/ https://%l:2381/
```

Web-launch aware tools and command line tools that always run on the CMS must be relative URLs beginning with `/`. For example,

```
/propertypages/Identify.jsp?device=%n
```

Multiple selections can be substituted into the URL. A selection index is used during the substitution process to track the *current* selection. The selection index is initially set to 1, and the first selection of the list of selected target systems remains current until a %z parameter is encountered in the URL. (An exception to this exists in the repeat block.) When the %z parameter is encountered, the next selection becomes current, the selection index is incremented by 1, and so on. For example,

```
http://server/app/doit.jsp?name=%n%z&addr=%a
```

where the *doit.jsp* page is invoked with the network name of the first selected system assigned to the *name* parameter and with the IP address of the second selected target assigned to the *addr* parameter.

You can substitute any number of selected targets by using the repeat block construct, `%( ... %)`. Anything inside the repeat block delimiters is repeated until the selection list is exhausted, starting with the current selection and selection index. For example,

```
https://%{deploy.server%}/deploy/deployimage.jsp?  
device1=%n%z%(&device%i=%n%z%)
```

NOTE: When using the `%i` parameter, the current selection index (1, 2, 3, and so on) is substituted for this parameter during the substitution process.

If the end of the repetition clause is reached and no `%z` parameter is encountered, the selection index and current election are automatically incremented to avoid an infinite loop during the substitution phase.

In the above example, if there were two selected target systems, the expanded URL string would look like this:

```
https://deploy.hp.com:280/deploy/deployimage.jsp?  
device1=nodea.hp.com&device2=nodeb.hp.com
```

If there was only one selected target system, the expanded URL string would look like:

```
https://deploy.hp.com:280/deploy/deployimage.jsp? device1=nodea.hp.com
```

Because there is no current selection when the string gets to the repeat block, the repeat block is suppressed during the substitution process.

Creating custom tools through the GUI

-
- ❗ **IMPORTANT:** Use of a single quote, `'`, inside a tool parameter field is not supported in the HP SIM GUI. However, you can use a double quote, `"`, instead.

Use the **Manage Custom Tools** page to view and manage custom tools created through the **New Custom Tool** feature. The **Manage Custom Tools** page displays a table listing the custom tools and information on each tool. The table includes:

- Selection column
- Name
- Description
- Command
- Run as user
- Automatic Event Handling

The following options are available for managing custom tools:

- “New” (page 83)
- “Edit” (page 83)
- “View tool definition” (page 84)
- “Run Now/Schedule” (page 84)
- “Delete” (page 84)

New

Use to create a custom tool and open the **Select the tool to create** page.

Edit

Use to edit an existing custom tool. Select the tool, and then click **Edit**. The **Edit Custom Tool Details** section appears. You can edit all fields and add or delete environment variables.

View tool definition

Use to display the XML code for the tool. This tool is not enabled if you select more than one tool.

Run Now/Schedule

Use to run the tool immediately or to schedule the tool to run (if the tool can be scheduled). If the tool can be run, the schedule a task page appears. You can schedule when and how often the tool runs.

Delete

Use to delete a tool. Deleting a tool removes it from the **Manage Custom Tools** page and from the system. If a tool is dependent on a task, an alert appears with the list of tasks associated with the tool.

For information custom tool definition files details, see [“Custom tool definition files”](#) (page 219).

Creating custom tools through the HP SIM CLI

HP SIM includes a CLI that allows manual control of HP SIM functions. This manual control enables you to create your own customized tools. The CLI is accessible directly on the CMS or from any network client using [SSH client](#) software. Creating custom tools manually offers a better understanding of the XML file format and allows greater flexibility in exercising the options available when creating TDEFs. For more information on custom tool definition file syntax, see [“Custom tool definition files”](#) (page 219).

Creating a custom SSA tool

This procedure uses the CLI to create a custom SSA tool for copying any executable file to a managed system (target system) and having it execute (install) there.

This example illustrates the creation of a custom tool that installs a security patch on every Windows server managed by HP SIM. If done manually, the administrator would have to locate each Windows server and perform the following commands in that server:

- Log on as Administrator
- Access a network drive or portable media containing a copy of the file to be used for the tool (we will use `hpsecurity_patch.exe` in this example) and copy that file to the local drive.
- Use Start/Run or a command line prompt to enter the command:
`<install_path>\hpsecurity_patch.exe`
- Log off of the system

For this example, it is assumed that the administrator will want to execute this procedure again and be able to quickly locate it in the HP SIM menus, so an entry in the **Deploy** menu is made and called **Software Distributor**, which when invoked allows the administrator to execute this custom tool.

Procedure 13 Creating the Software Distributor tool

1. Log into the CMS using a valid user name and password. HP SIM grants authorization based on the operating system login.

NOTE: Only administrators have command line access to HP SIM on a Windows CMS. Administrators on a HP-UX/Linux CMS must have root capability.

2. Open a terminal window or a command prompt window to execute HP SIM commands.
3. Open a text editor and create a new file by typing the XML version text and tool list tags as follows:

```
<?xml version="1.0" encoding="UTF-8" ?>
<tool-list>
```

NOTE: Your text editor must be able create a text-only file with no embedded formatting.

- Following the leading XML version and tool-list tags, type the tool name tag of `<ssa-command-tool name=<Deploy HP Security Patch>` to define the type and name of the tool. The revision string is used to keep track of different versions of the tool as will be seen later. Enter the subsequent category, description, and comment elements to further define the tool for HP SIM and the user (the description and comments will be displayed in the GUI window for that particular tool).

```
<?xml version="1.0" encoding="UTF-8" ?>
<tool-list>
  <ssa-command-tool name="Deploy HP Security Patch" revision="1.0">
    <category>Software Management</category>
    <description>Deploy HP Security Patch v.1 to the target
node</description>
    <comment>This tool will deploy hpsecurity_patch.exe to the
target Node. Please verify that the hpsecurity_patch.exe is located in
C:/temp before deploying.</comment>
```

- Enter the `execute-as-user` element with the value of `Administrator` to define the user whose permissions are allowed on the target node. After entering the `execute-as-user` element, the TDEF should display as follows:

```
<execute-as-user>Administrator</execute-as-user>
```

- The `include-filter` element specifies which hardware and/or operating system filters will be applied. For this example, enter the `include-filter` data as shown below.

```
<include-filter type="os">
  <node-filter name="OSName" operator="eq"
value="WINNT" />
</include-filter>
```

- Following the `include-filter` element is a `block` element that is the heart of the tool and includes the command(s) to be executed. Enter the `ssa` block element as shown below. It will copy the file to the specified destination and execute it there. In the example, the HP Security Patch v.1 executable is given the filename `hpsecurity_patch.exe`.

```
<ssa-block>
  <command command-type="stdout" log="false">C:\\Program
Files\\hpsecurity_patch.exe</command>
  <copy-block>
    <source>C:\\temp\\hpsecurity_patch.exe</source>
    <destination>C:\\Program
Files\\hpsecurity_patch.exe</destination>
  </copy-block>
</ssa-block>
```

NOTE: The `<destination>` must be a directory that exists on the Managed Node. The default file permission value used by DTF for a file copy operation is 755. If another permission is to be used, an explicit file permission command such as `chmod` should be included in the copy block element for security reasons.

8. Type the following attribute element code, which states where the tool will be located in the HP SIM menu.

```
<attribute name="menu-path">Deploy|Software Distributor</attribute>
```

9. To finish the TDEF, enter the final tool list tag as shown below.

```
</tool-list>
```

The fully composed TDEF for a SSA copy tool to deploy the HP Security Patch to a managed node and then execute, should display as follows:

```
<?xml version="1.0" encoding="UTF-8" ?>
<tool-list>
  <ssa-command-tool name="Deploy HP Security Patch"
revision="1.0">
    <category>Software Management</category>
    <description>Deploy HP Security Patch v.1 to the target
node</description>
    <comment>This tool will deploy hpsecurity patch.exe to
the target Node. Please verify that hpsecurity patch.exe is located
in C:/temp before deploying.</comment>
    <execute-as-user>Administrator</execute-as-user>
    <include-filter type="os">
      <node-filter name="OSName" operator="eq"
value="WINNT" />
    </include-filter>
    <ssa-block>
      <command command-type="stdout"
log="false">C:\\Program Files\\hpsecurity patch.exe</command>
      <copy-block>
        <source>C:\\temp\\hpsecurity patch.exe
        <destination>C:\\Program Files\\
hpsecurity patch.exe</destination>
      </copy-block>
    </ssa-block>
    <attribute name="menu-path">Deploy|Software
Distributor</attribute>
    <attribute name="i18n-attrs">TOOL,mxtools</attribute>
  </ssa-command-tool>
</tool-list>
```

10. Save the file. HP recommends using a file name that indicates its function, in this case, DeployHPSecurityPatchv.1.xml. Make sure that the file name ends with the .XML extension. Note that file names on Linux and HP-UX operating systems are case-sensitive. The directory used by HP SIM to store tools is as follows:
 - for HP-UX and Linux systems: /var/opt/mx/tools
 - for Windows systems: C:\\Program Files\\HP\\Systems Insight Manager\\tools
11. To add the new tool to HP SIM, perform the procedure described in the section [“Adding a TDEF to HP SIM”](#) (page 89).

For more information about specific SSA tool attributes, see [“SSA-specific attributes”](#) (page 219).

Example Web launch tool

A web launch tool launches an application requiring a URL. The example below launches the application **WebJetAdmin** for a device selected within the HP SIM window as long as that device is a printer. The `<web-block>` element (in bold below) provides the URL of the managed node where **WebJetAdmin** is installed. The parameter `%n` is used to substitute the managed node hostname. The `<toolbox-enabled>` element can have a value of true or false. If the `<toolbox-enabled>` element is true, it will be associated with the **Toolboxes** under **HP SIM User and Authorization**. This allows a trusted user to disable the tool in the **Toolbox** if the value is false. This tool launches in a separate browser window using the "target-frame" of WJAFrame. For additional parameters, see ["mxtool command parameters" \(page 221\)](#).

```
<?xml version="1.0" encoding="UTF-8" ?>
<tool-list>
  <web-launch-tool name="WebJetAdmin" max-targets="1" revision="1.0">
    <category>Local Tools</category>
    <description>View properties of remote printer via
WebJetAdmin.</description>
    <execute-as-user>root</execute-as-user>
    <toolbox-enabled value="true" />
    <include-filter type="hardware">
      <node-filter name="DeviceType" operator="eq" value="Printer"/>
    </include-filter>
    <web-block accepts-targets="true">
      <main-url>http://hostname.domain:8000/device/%n</main-url>
    </web-block>
    <attribute name="menu-path">Tools|System Information</attribute>
    <attribute name="target-frame">WJAFrame</attribute>
  </web-launch-tool>
</tool-list>
```

NOTE: In the previous example, `hostname.domain` should be replaced with the FQDN of where the WebJetAdmin tool is running.

For more information about specific web launch tool requirements and attributes, see ["WLA-specific attributes" \(page 220\)](#). For more information about parameterized strings, see ["Parameterized strings" \(page 221\)](#).

Example MSA tool

The MSA tool executes on the CMS and is functional with multiple targets. The process executes once, and then is passed to all targets selected. The example below shows an MSA tool that deploys the SSH [public key](#) to the selected managed target nodes as long as those nodes are recognized as iLO devices on an HP single partition server. To do this manually, the administrator would:

- Log on as Administrator on the CMS
- Use Start/Run or a command line prompt to enter the command.
- `mxagentconfig -a- n nodename -u username -p password`
- Repeat the command for each managed system
- Log off the system

The `<msa-block>` element (in bold below) initiates `mxagentconfig` and requires the user name and password parameters.

NOTE: When the XWindows tool is launched, the system running the browser must be running an XWindows server for the tool's GUI to be visible.

```

<?xml version="1.0" encoding="UTF-8" ?>
<tool-list>
  <msa-command-tool name="Deploy SSH Public Key" visible="true"
    schedulable="true" revision="2.1">
    <category>MP Tools</category>
    <description>Deploys the HP Systems Insight Manager SSH public key on
      one or more HP Integrity and HP 9000 iLO(s). This key is required
      for iLO to trust HP Systems Insight Manager to execute
      commands.</description>
    <comment>Install SSH Public Keys</comment>
    <include-filter type="hardware">
    <node-filter name="DeviceType" operator="eq" value="MgmtProc" />
    <node-filter name="Model" operator="eq" value="HP Single Partition
      Server, Management Processor" />
    </include-filter>
    <msa-block>
    <command command-type="stdout" log="true">mxagentconfig -a %( -n
      %n%z%) -u %1 -s %2</command>
    <parameter index="1" prompt="User" required="true" />
    <parameter index="2" prompt="Password" required="true" />
    <execution-node>CMS</execution-node>
    </msa-block>
    <attribute name="insert-separator">true</attribute> <!-- Optional -->
    <attribute name="custom-page-
      1">/taskandjob/MpTools/MpInstallSSHKeyCPP1.jsp</attribute> <!--
      Optional -->
    <attribute name="menu-path">Configure </attribute>
    <attribute name="menu-sort-key">800</attribute> <!-- Optional -->
    <attribute name="i18n-attrs">TOOL,mxtools</attribute>
    <attribute name="show-cmdline">>false</attribute>
    </msa-command-tool>
  </tool-list>

```

For more information about specific MSA tool requirements and attributes, see [“MSA-specific attributes”](#) (page 219).

Example Enabling Remote Desktop tool

Remote Desktop is a Microsoft feature that enables you to remotely access any Windows 2003 server. Unfortunately, Remote Desktop is disabled by default during installation, which can lead to problems accessing the system without physically being present in front of the server. HP SIM enables you to create a custom TDEF to enable remote desktop on selected targets as long as the selection is running Windows 2003 server operating system. The following example demonstrates the ability of the TDEF to create a menu item called **Enable Remote Desktop**.

```
<?xml version="1.0" encoding="UTF-8" ?>
<tool-list>
  <ssa-command-tool name="Enable Remote Desktop" revision="1.0">
    <category>Software Management</category>
    <description>Change the registry value from 1 to 0 to enable
remote desktop</description>
    <comment>The tool can be run on multiple Windows
systems</comment>
    <execute-as-user>Administrator</execute-as-user>
    <include-filter type="os">
      <node-filter name="OSName" operator="eq" value="WINNT"
/></include-filter>
    <ssa-block>
      <command command-type="stdout" log="false">reg add
"hklm\system\currentcontrolset\control\terminal server" /f /v
fDenyTSCconnections /t REG_DWORD /d 0</command>
    </ssa-block>
    <attribute name="menu-path">Configure</attribute>
    <attribute name="i18n-attrs">TOOL,mxtools</attribute>
  </ssa-command-tool>
</tool-list>
```

Adding a TDEF to HP SIM

After you create a custom TDEF, to function, you must add it into HP SIM. Add a TDEF to HP SIM using the `mxtool -a` command, as described in the following procedures:

Procedure 14 Adding a TDEF to HP SIM

1. At a terminal or command line prompt, type `mxtool -a -f <file pathname> .`

NOTE: For more information about `mxtool` command parameters, see [“mxtool command parameters” \(page 221\)](#).

2. To use the web launch tool previously created, type:

```
mxtool -a -f /tools/webjetadmin.xml
```

A successful TDEF addition results in a dialog box displaying the following

```
Successfully parsed tool file
```

```
Successfully added tool named "WebJetAdmin"
```

```
Successfully added 1 tool
```

Removing a TDEF from HP SIM

Removing a TDEF from HP SIM requires using the option `-r` when running the `mxtools` command.

Removing a tool is not OS specific and can be run from a terminal or command prompt.

To remove a TDEF from HP SIM, use the `mxtool -r` command as in the following example:

Procedure 15 Removing a TDEF from HP SIM

1. `mxtool -r -f /tools/webjetadmin.xml`
2. A successful TDEF removal will result in the dialog box displaying the following:

```
Successfully parsed tool file
```

```
Successfully removed tool named "WebJetAdmin"
```

```
Successfully removed 1 tool
```

NOTE: If a task or task results are tied to a tool, by default the tool cannot be removed. The `-x` force option is used in this case.

Modifying a TDEF

Modifying a TDEF allows users to customize the XML to align with their business. Each TDEF included can be modified to fit with each customers business needs.

To modify a TDEF to execute as a different user, perform the following steps:

Procedure 16 Modifying a TDEF

1. Modify the Windows HP SIM tools to use the new user account as follows:
 - a. Navigate to the tools directory.
Example: `C:\Program Files\HP\HP SIM\tools`
 - b. Search the tools directory for the tool to modify. Alternatively, you may create a tool definition file from an existing tool using the `mxtool` command.
Example: `mxtool - lf -t netstat > netstat.xml`
 - c. Edit `netstat.xml` using a text editor. Find each `execute-as-user` line in the XML file.
Example: `<execute-as-user>Administrator</execute-as-user>`
 - d. (Optional) Change the revision attribute value for the tool type and name element or use the `-x force` option on the `mxtool` command line:
Example: In the SSA command tool sample code in the previous example, change `revision="1.0"` to `revision="1.1"`.
 - e. Run `mxtool` to update the tool definition:
Example: `mxtool -m -f netstat.xml -x force.`
2. Configure each managed system that is to run tools with the user account. If the current user account was used to install OpenSSH, then the managed node should be correctly configured. If a different account is used, then the administrator should either run the **Configure or Repair Agents** tool on the systems (specifying the administrator or other account to be used by the SSH), or perform the following steps:
 - a. Add the administrator user to the `passwd` file using the "sshuser" utility on the managed system. Example: `sshuser -u MyUser -d MyDomain -f "C:\Program Files\OpenSSH\etc\passwd"`
 - b. Run `mxagentconfig` on the CMS to configure public key authentication for the administrator user. Example: `mxagentconfig -a -n <managed system> -u MyDomain\MyUser`

NOTE: For more information about `mxtool` command parameters, see [“mxtool command parameters” \(page 221\)](#).

To view changes to TDEFs, refresh the HP SIM GUI by selecting the system list. A software restart is not necessary.

18 Federated Search

Select **Reports**→**Federated Search**....

Federated Search is a web-based HP SIM plug-in that enables you to search quickly across a number of Systems Insight Manager CMS systems. Federated Search finds systems using basic system criteria such as name, system type, subtype, and operating system. The search tool can also search software inventory information to find, for example, firmware versions across all Windows systems. From the search results, you can drill down into specific systems on specific CMSs, accessing all features on those CMSs and you can have the results exported to CSV, a comma-separated value, format. Advanced search can also be performed.

How it works

- System administrators log into the host CMS running the Federated Search tool and launch the tool from the HP SIM **Reports** menu.
- A list of searchable CMSs appears with their respective connection status, version information, and system counts.

NOTE: Federated Search must be configured before a search can be performed.

- Submit search criteria (name, status, system type/subtype, product, operating system) and the Federated Search UI searches other CMSs through their respective HP SIM web service APIs.
- Other CMSs in the organization returns the individual search results in a single table.

Federated CMS Configuration

The Federated CMS Configuration feature provides you with the following options:

- **Adding a CMS**
A wizard guides you through the process of adding a CMS.
- **Deleting a CMS**
A selected CMS can be removed from the list of CMSs. When the CMS is deleted, the trust relationship that was set up between the main CMS and secondary CMS is also removed.
- **Refreshing the list**
Refreshing the list re-checks the configurations from the CMS.
- **Fixing the configuration of a CMS**
After the initial configuration of a CMS, changes in the CMS could break the Federated CMS configuration. The CMS table displays the current configuration status since the last refresh. If the configuration is broken, you must use **Fix CMS Configuration** to repair the configuration.

Procedure 17 Adding a CMS

1. Click **Add CMS**. The **Add CMS** wizard appears.
2. Enter the name of the remote CMS using the host name or IP address.
3. Verify the SSL certificate from the remote CMS.

This step gets the SSL certificate from the secondary CMS and allows you to install it on the main CMS. If the certificate is retrieved successfully, it is displayed. After viewing the certificate, you can click **Finish** or **Cancel** the wizard. If you finish the wizard, the certificate is installed.

NOTE: Any time communication with a secondary CMS is initiated, the certificate returned must already be installed.

4. Configure the remote CMS.

The main CMSs SSL certificate is exported to the secondary CMS, and the secondary CMS is configured to trust the main CMS. To have this configuration performed, you must provide credentials for a full-rights HP Systems Insight Manager user on the secondary CMS. The credentials supplied are used for this one transaction and are not permanently stored.

NOTE: To avoid remote CMS connection errors, make sure a firewall is not blocking ports 50001 and 50002 on the remote CMS.

See the HP Systems Insight Manager online help for additional information.

19 CMS Reconfigure Tool

The CMS Reconfigure Tool feature provides a set of commands that enable you to quickly make common reconfiguration changes to HP SIM, HP Insight Control, HP Virtual Connect Enterprise Manager, and HP Matrix OE.

The challenge in attempting to make operating system or CMS configuration changes is the difficulty in knowing exactly what steps need to be performed on a particular operating system/CMS installed environment. The `mxreconfig` command fills the need for an automated application tool to perform these tasks for the Insight Management software components.

The CMS Reconfigure Tool is supported through HP SIM and only on systems running Microsoft Windows with SQL server.

Prior to executing any CMS Reconfigure Tool command, ensure the CMS and associated database are backed up. For information about backing up the CMS, see the *Backing up and restoring HP Insight Software Central Management System (Windows)* white paper at: <http://www.hp.com/go/insightmanagement/sim/docs>.

Operational Commands, Options and Parameters

Operational command type options for `mxreconfig` are those designated single-char options that must be the first option placed on the entered command line string. These type options may or may not require an additional argument string. For example, the operational command option `-m` (*mode*) requires an argument. This operational option is used to specify a particular reconfiguration mode. The required associated argument string identifies which specific reconfiguration task mode needs to be performed in the specified mode, such as `host` (to change host name) or `password` (to change password).

An example of an `mxreconfig` command is shown below. This command is a request to change the CMS host name (additional command line options and arguments would be required for this particular reconfiguration command and are described later).

```
>mxreconfig -m host
```

An example of an operational command option that does not require an argument is the `-h` (*help*) option. This operational option is used to show brief online help usage text in the console. No associated argument string is required.

```
>mxreconfig -h
```

Parameter type options are those single-char options that follow the operational command option on the entered command line string. These type options may be required or may be optional for the specified operational command option being given, and the parameter option itself might not require an additional argument string. An example of using a parameter type option is the `-a` option which is used to specify the database user name. This particular type parameter option does require an additional string argument, which is the actual specified database username.

```
>mxreconfig -m dbauth -a db-username-here
```

The usage of the available commands depends on the products you have installed. See the *HP Systems Insight Manager Command Line Guide* at <http://www.hp.com/go/insightmanagement/sim/docs>, for information on the command options, arguments, and parameters.

Reconfiguring the CMS password

The `mxreconfig -m password` command prompts you for a new password and changes the credentials configured. The `mxreconfig -m password` command realigns the Insight Management software services account credentials with the operating system password (after this has been changed). If the user that installed Insight Management software changes the Windows logon password, then that user must also run this command to make Insight Management software match the new operating system password.

When this command is run, and the new password is typed and confirmed, all services are stopped. The password entered is then updated on services that are configured to run using the installing user's credentials. Services running as local system will not be changed.

NOTE: This command does not work with HP Insight Control server deployment. See the *HP Insight Control Server Deployment User Guide* for more information.

Dependencies

- HP SIM, HP Insight Control, HP Virtual Connect Enterprise Manager, or HP Matrix OE are installed and configured on a Windows operating system, using Microsoft SQL.
- The user changed their password in the operating system using standard Windows password change tools.

NOTE: If you have HP Insight Control server deployment installed, you must update the credentials it uses by following the **Changing deployment server/solution username or password (after initial installation)** section in the *HP Insight Control Server Deployment User Guide*.

Warnings

Verify that all jobs related to HP SIM, HP Insight Control, HP Virtual Connect Enterprise Manager, and HP Matrix OE are complete before running this command. If HP System Management Homepage is open, close it.

Changing the CMS password

Procedure 18 Changing the CMS password for HP SIM and Insight Control

1. Open a command prompt on the CMS.
2. Enter the following and then press **Enter**:
`mxreconfig -m password`
3. Enter the new password (characters are hidden), and then press **Enter**.
4. When prompted to confirm the password, enter the new password again, and then press **Enter**.
5. You must authorize the new password with the old password. Enter the old password, and then press **Enter**.
6. The utility stops the HP SIM, HP Insight Control, HP Virtual Connect Enterprise Manager, and HP Matrix OE services, changes the password, and then restarts the services.
7. If the CMS is associated with a locally installed SQL database, and the SQL database services are running with the same user authentication, then update the SQL services login credential with the new password.
8. If the associated SQL database is remote, then you must also follow to run the `mxreconfig -m dbauth` command.

Procedure 19 Changing CMS password for Matrix OE and Operations Orchestration

1. Execute the following commands from the command prompt:
`mxpassword -m -x MxDBUserPassword=<New Password>`
`mxpassword -m -x io.db.password=<New Password>`
`mxpassword -m -x oo.admin.password=<New Password>`
2. Update the `gwlmdb.properties` file by executing the following command from the command prompt:
`vseinitconfig -a`

3. Open the Windows command prompt and navigate to `..\Program Files\HP\Operations Orchestration\Central\tools`.
 4. Execute `change-db-props.bat` to change the Operations Orchestration database password. Enter the following and press **Enter**:

```
C:\Program Files\HP\Operations Orchestration\Central\tools>change-db-props.bat <db-user-name><New password>
```

The command, `change-db-props` must be executed passing **only** the user name and not domain, even if this is a domain account.
 5. Restart the RSCentral Windows service.
The RSCentral service must be updated to use the user and password for changed account (not the local account). Service must run with credentials that has access to the database.
 6. Open Operations Orchestration Central (Web portal) at `https://localhost:16443/PAS/` and log in using the old (unchanged) credentials.
-
- NOTE:** If the Web portal does not open after Step 5, verify that the RSCentral service is running under the new credentials; if not, update the service logon credential with the new password and repeat from Step 4.
-
7. Select the **Administration** tab and change the password for the admin user. The new admin password must match the `oo.admin.password` specified in Step 1.

Reconfiguring the CMS host and IP attributes

The `mxreconfig -m host` command enables you to realign the CMS host name and/or IP address with the operating system after the operating system host name and/or IP address has changed. For example, this command could be used after renaming the server on which HP SIM is installed.

The host command does the following:

- Stops all installed HP SIM and Insight Control services.
- Updates references to the CMS host name.
- Updates CMS primary IP address.
- Creates a new CMS certificate.
- Starts all installed HP SIM and Insight Control services.

NOTE: If the SQL database associated with the CMS is installed locally (on the same server), and you have changed the host name and/or IP address, you must run `mxreconfig -m sqlredirect` before running `mxreconfig -m host -c <OldCmsName>`.

Where:

- **-c <OldCmsName>**
Old name of the CMS.

NOTE: If you configured sites in Matrix Recovery Management, an additional step must be applied:

Run the `mxreconfig -m host -c <OldCmsName>` command.

The Matrix Recovery Management (MRM) updates the local Central Management Server name to the current local hostname. You need to change the MRM remote CMS name on the peer (remote) CMS as well. See the *MRM Online Help* for editing sites.

Known limitations:

- HP EVA storage array is not supported if the local hostname is changed with the `mxreconfig` command
-

Dependencies

- HP SIM, HP Insight Control, or Matrix Operating Environment is installed and configured on a Windows operating system host, using Microsoft SQL.
- The host name for the operating system was changed using standard Windows configuration tools.
- The host is still in the same domain.
- All credentials are known.
- The new host name can be resolved by the DNS server.
- The new IP address is valid (assigned through DHCP if enabled on the CMS) and is the IP address assigned to the CMS.
- If the SQL database is a local database running on the CMS server, reconfigure the CMS database information using the `sqlredirect` command.

Warning

Verify that all HP SIM or HP Insight Control operations are complete before running this command.

Reconfiguring the CMS host name and primary IP address

To reconfigure the CMS host name and primary IP address, complete the following:

Procedure 20 Reconfiguring the CMS host name and primary IP address

1. Open a command prompt on the CMS and navigate to the install directory of HP SIM.
2. Type the following, and then press **Enter**:
`mxreconfig -m host`
3. Follow the prompts that appear to complete the host name and IP address change.

Reconfiguring the CMS database credentials

The `mxreconfig -m dbauth -a <dbuserDomain\dbuser>` command enables you to change the credentials used by Insight Management to access the CMS database. If the user name

used to logon to the database associated with Insight Management software must be changed, then this command must be used.

Dependencies

- CMS is installed and configured on a Windows operating system host, using Microsoft SQL.
- All credentials are known.
- The database credentials provided by the user during this command are valid for the CMS database.

Warning

Verify that all Insight Management software operations are complete before running this command.

Changing the HP SIM and HP Insight Control database credentials

Additional steps are required to change the database authorizations for Matrix OE and Operations Orchestration:

Procedure 21 Changing the HP SIM and HP Insight Control database credentials

1. Open a command prompt on the CMS and navigate to the install directory of HP SIM.
2. Type the following, and then press **Enter**.

```
mxreconfig -m dbauth -a <db-user-name>
```

3. Enter the new password when prompted, and then press **Enter**.

Changing the database authorizations for Matrix OE and HP Operations Orchestration

Additional steps are required to change the CMS password for Matrix OE and Operations Orchestration:

Procedure 22 Changing the database authorizations for Matrix OE and HP Operations Orchestration

1. Update the `gwlmdb.properties` file by executing the following command from the command line:

```
vseinitconfig -a
```

2. Open a Windows command prompt and navigate to `..\Program Files\HP\Operations Orchestration\Central\tools`.
3. Execute the following commands from the command prompt:

```
mxpassword -m -x MxDBUserPassword=<New Password>
```

```
mxpassword -m -x io.db.password=<New Password>
```

4. Execute `change-db-props.bat` to change the Operations Orchestration database password. Type the following and press **Enter**:

For example:

```
C:\Program Files\HP\Operations Orchestration\Central\tools>change-db-props.bat <dbuser> <New password>
```

The command, `change-db-props` must be executed passing only the user name and not domain, even if this is a domain account.

5. Update `jdbc.properties` file located under `IO_install_directory\conf`. Update the following line:

```
jdbc.username = <new_user>
```

6. Update chargeback service `jdbc.properties` file located under `IO_install_directory\chargeback\conf`. Update the following line:

```
jdbc.username = <new_user>
```

NOTE: If HP Capacity Advisor Data Service is not running after executing `dbauth`, you must update the hosts file under `Windows\System32\drivers\etc` and add `<cms_name>`, where `<cms_name>` is the hostname of CMS. Be sure to save the file and restart HP Capacity Advisor Data Service if it was stopped.

Reconfiguring the CMS to use a different database

Use the `mxreconfig -m sqlredirect -s <dbserver> -b <dbname> -a <dbuserDomain\dbuser> [-p <dbport>]` command to reconfigure the CMS to use a different database.

Where:

- **-a <dbuser>**
Name of the database user with administrative privileges, must include domain name.
- **-b <dbname>**
Name of the new database.
- **-s <dbserver>**
Name of the new database server
- **-p <dbport>**
Port number to access the new database server

This command updates the CMS to associate itself with a new Microsoft SQL database residing on a different server. If the database previously associated with HP SIM or HP Insight Control must be changed, use this command to specify the new database server and database name. You can optionally specify the database port number on which HP SIM or HP Insight Control communicates with the new database, and the username credential that HP SIM or HP Insight Control uses to access the new database.

NOTE: This is not supported on VCEM or Matrix Operating Environment.

NOTE: The parameters `-s`, `-a` and `-b` and their arguments are required. The parameter `-p` and its argument is optional.

This command does the following:

- Stops all installed HP SIM or HP Insight Control services.
- Redirects the CMS to use the new SQL database.
- Modifies the CMS configuration files to reflect the new SQL server name.
- Restarts all installed HP SIM or HP Insight Control services.

Dependencies

- The database to be associated with HP SIM or HP Insight Control has been copied and setup on a different SQL server.
- HP SIM or HP Insight Control is installed and configured on a Windows operating system, using Microsoft SQL.

Warning

Verify that all HP SIM or HP Insight Control operations are complete before running this command.

Changing the database associated with the CMS

To change the database associated with the CMS, perform the following:

Procedure 23 Changing the database associated with the CMS

1. Open a command prompt on the CMS and navigate to the install directory of HP SIM.
2. Type the following and then press **Enter**.

```
mxreconfig -m sqlredirect -s <dbserver> -b <dbname> -a  
<dbuserDomain\dbuser>
```

Where:

- **-a <dbuser>**
Name of the database user with administrative privileges, must include domain name.
- **-b <dbname>**
Name of the new database.
- **-s <dbserver>**
Name of the new database server

3. Enter the database password when prompted, and then press **Enter**.

20 Understanding HP SIM security

This chapter provides an overview of the security features available in the HP SIM framework. HP SIM runs on a CMS and communicates with managed systems using various protocols. You can browse to the CMS or directly to the managed system.

Securing communication

Secure Sockets Layer (SSL)

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide communication security. It provides encryption to prevent eavesdropping, data integrity to prevent modification, and authentication for both client and server, leveraging public-key technology.

All communications between the browser and the CMS are protected by SSL. HP SIM supports SSLv3.0 and TLS 1.0 and uses stronger cipher suites, by default, for the web and the SOAP services. However, the list of ciphers could be configured to suit the security needs. For more information, see “[How to configure ciphers](#)” (page 100). Also note that HP SIM does not enforce stronger cipher suites for the WBEM indication receiver.

How to configure ciphers

Starting with version 7.2, HP SIM is capable of supporting user-defined ciphers to suit security needs. While the default set of ciphers are limited to the ones available in the JRE, it can be extended to support higher strengths by downloading and configuring Java Cryptography Extensions (JCE) on top of the JRE distributed with HP SIM. For more information, see <http://www.oracle.com/technetwork/java/javase/downloads/jce-6-download-429243.html>.

1. Use the `mxcipher -d` CLI command to view the existing ciphers configured in HP SIM.
2. Use the `mxcipher -e` CLI command to change the ciphers to suit your security needs.

For more information, see the *HP Systems Insight Manager CLI Guide* at <http://www.hp.com/go/insightmanagement/sim/docs>.

Secure Shell (SSH)

SSH is an industry-standard protocol for securing communications. It provides for encryption to prevent eavesdropping plus data integrity to prevent modification, and it can also authenticate both the client and the server utilizing several mechanisms, including key-based authentication. HP SIM supports SSH 2.

Hyper Text Transfer Protocol Secure (HTTPS)

HTTPS refers to HTTP communications over SSL. All communications between the browser and HP SIM are carried out over HTTPS. HTTPS is also used for much of the communication between the CMS and the managed system.

Secure Task Execution (STE) and Single Sign-On (SSO)

STE is a mechanism for securely executing a command against a managed system using the Web agents. It provides authentication, authorization, privacy, and integrity in a single request. SSO provides the same features but is performed when browsing a system. STE and SSO are implemented in very similar ways. SSL is used for all communication during the STE and SSO exchange. A single-use value is requested from the system prior to issuing the STE or SSO request to help prevent against replay or delay intercept attacks. Afterwards, HP SIM issues the digitally signed STE or SSO request. The managed system uses the digital signature to authenticate the HP SIM server. Note that the managed system must have a copy of the CMS SSO certificate imported into the

Web agent and be configured to trust by certificate to validate the digital signature. SSL can optionally authenticate the system to HP SIM, using the system's certificate, to prevent HP SIM from inadvertently providing sensitive data to an unknown system.

NOTE: For SSO to web agents, the Replicate Agent Settings and Install Software and Firmware tools each provide administrator-level access to the web agents. HP System Management Homepage As Administrator, System Management Homepage As Operator, and System Management Homepage As User each provide SSO access at the described level.

Distributed Task Facility (DTF)

DTF is used for custom command tools and multiple- and single-system aware tools. Commands are issued securely to the managed system using SSH. Each managed system must have the CMS SSH public key in its trusted key store so that it can authenticate the CMS. Managed systems are also authenticated to the CMS by their SSH public key.

In HP SIM, the Privilege Elevation feature enables tools to be run against HP-UX, Linux, and ESX managed systems by first signing in as a non-root user, and then requesting privilege elevation to run root-level tools. This can be configured under **Options**→**Security**→**Privilege Elevation**.

WBEM

All WBEM access is over HTTPS for security. HP SIM is configured with a user name and password for WBEM agent access. Using SSL, HP SIM can optionally authenticate the managed system using its SSL certificate.

For HP-UX, certificates can be used instead of username and password for WBEM authentication. You can configure WBEM authentication from the **System Credentials**→**WBEM** tab by selecting **Options**→**Security**→**Credentials**→**System Credentials**. For more information, see the HP SIM online help.

LDAP

When configured to use a directory service, HP SIM can be configured to use LDAP with SSL (default) or without SSL, which would transmit credentials in clear-text. To enable LDAP over SSL in Microsoft Active Directory, refer to <http://support.microsoft.com/default.aspx?scid=kb;en-us;321051>. Additionally, the directory server can be authenticated using the Trusted Certificate list in HP SIM.

RMI

Java RMI is secured by requiring digitally signed requests using the CMS [private key](#), which should only be available to the local system. All communications use localhost to prevent the communication from being visible on the network.

Credentials management

SSL certificates

There are several certificates used by HP SIM.

HP SIM main certificate

The HP SIM main certificate is used by the HP SIM SSL web server, the partner application SOAP interface, and the WBEM indications receiver. This certificate is used to authenticate HP SIM in the browser, in partner applications that communicate with HP SIM through SOAP, and in WBEM agents that deliver indications to HP SIM.

By default the SIM main certificate is self-signed. Public Key Infrastructure (PKI) support is provided so that the main certificate may be signed by an internal certificate server or by a third-party [Certificate Authority](#) (CA). HP SIM suggests and supports certificate key sizes with 2,048-bit or

higher. In the case of fresh install scenarios, the HP SIM certificate will be a 2,048-bit self-signed certificate.

HP SIM SSO certificate

For Single Sign-On operations, HP SIM uses SSO certificate only; this is the self-signed 1,024-bit certificate. HP SIM does not support any other third party certificate or CA-signed certificate for SSO.

NOTE: Though the 2,048-bit certificate is suggested by HP SIM, since not all managed systems support it, HP SIM uses 1024-bit certificate for SSO, especially considering backward compatibility and upgrades.

WBEM certificate

In HP SIM 7.0 and later, the WBEM certificate uses the 2,048-bit key length. A new HP SIM 7.0 or later installation creates a WBEM certificate with the 2,048-bit key length. The WBEM certificate can be regenerated if required with the following commands:

```
mxcert -w(Distinguished Name)
```

```
mxcert -W
```

Upgrading to HP SIM 7.2

The HP SIM main certificate is automatically upgraded to a 2,048-bit self-signed certificate, if the previous certificate is a self-signed 1,024-bit certificate. However, if the previous certificate is a 2,048-bit certificate or above or it is a CA-signed certificate, HP SIM will retain the existing certificate and will not recreate a new certificate. Also, you may need to import the trusted certificates back into HP SIM's trust store.

The HP SIM SSO certificate is created if, and only if, there is no prior SSO certificate.

NOTE:

- An SSO certificate is used by HP SIM 7.0 and later. Therefore, there is a possibility that the previous version of HP SIM may not contain an SSO certificate. Only in these cases, the SSO certificate will be created during the upgrade process.
- Once the SSO certificate is created, the trust relationship with the managed systems must be re-established, by importing the new SSO certificate into the managed systems.

The HP SIM WBEM certificate is a self-signed 2,048-bit certificate and will not be overwritten upon upgrade to HP SIM 7.2.

Certificate expiration and Certificate Revocation Check (CRL Check)

HP SIM provides the support for certificate revocation check. By default, the revocation check is enabled for both client and server certificates. However, server certificates are checked for revocation only if you have enabled **Require Trusted Certificate** (**Options**→**Security**→**Credentials**→**Trusted Systems**→**Trusted Certificates**).

The Certificate revocation check can be configured from the GUI by selecting **Options**→**Security**→**Certificate Revocation Configuration Check**.

You can also configure certificate revocation check by entering: `mxcert -L` from the command line.

Source of client and server certificates

The client certificates are sent to HP SIM by the Web portal, partner requests, and the WBEM services.

The server certificates are sent to HP SIM by the managed systems.

Enabling or disabling certificate revocation check

HP SIM enables you to disable certificate revocation check for both server and client certificates. Disabling revocation check for client certificate does not affect Two-Factor authentication, where the client certificate (called as user certificate) is always checked for revocation.

Enabling certification revocation check might affect the performance of the system as it downloads the Certificate Revocation List (CRL) file from the certificate server during the processing of revocation check. The downloading of the CRL file happens only if a CRL file associated with the certificate is not already cached in the server, or CRL file that is cached is expired.

Enabling or disabling certificate revocation check does not require restart of HP SIM.

Offline and online mode of certificate revocation check

The certificate revocation check is performed offline and/or online.

Offline mode

The offline mode is set as the default mode of checking the revocation. The offline mode expects the CRL files to be cached in the system. You must regularly populate the CRL files associated with the certificates in a directory maintained by HP SIM. In Windows, the directory is `\data\crl`, and in Linux/HP-UX, this directory is `/var/opt/mx/data/crl`.

Alert on CRL file expiration

If any of the CRL files present in this directory are expired, then HP SIM will send an alert to the System. These alerts could be seen in "All Events" page.

The intent of this alert is to inform User to update the CRL directory with the latest CRL files.

Please see below to configure few of the CRL alert related settings.

Online mode

The online mode can optionally be enabled. Enabling online mode does not bypass the offline mode of CRL check.

If the CRL file associated with a certificate is not present in the above directory, or if the cached CRL file is expired, then HP SIM checks if online mode has been enabled. If online mode is enabled, HP SIM tries to download the CRL file from the certificate server. After downloading the CRL file, HP SIM caches the file in the above directory.

Ways of enabling online mode

There are two ways of enabling online mode. One is through Proxy settings, and the other is directly.

In the former method, you must save the host address and the port of the proxy server.

The latter method assumes that the certificate server is reachable from the CMS server without the need for the proxy settings. Example, the certificate server is located in the same intranet as the CMS server.

In the future, the proxy settings will be configured in a common location in HP SIM.

CRL distribution points

HP SIM expects the CRL distribution points to be present in the certificate and the CRL distribution point URLs are valid. There is a possibility that revocation check might fail if any of the distribution points contains an invalid URL.

HP SIM processes only HTTP distribution point URLs. If a certificate does not contain a HTTP distribution point URL, then the CRL check for the certificate will fail.

Warning or error

If the certificate revocation check cannot be performed successfully, then HP SIM logs that as a warning, but it does not cease the connection with the peer system. The connection will be ceased only if HP SIM identifies the certificate as revoked.

In Two-Factor authentication, if the revocation check did not succeed or if the certificate is revoked, then the user is not allowed to log-in to the CMS.

Conditions for warning

- If the CRL distribution point is not available in the certificate
- If the CRL distribution point does not contain HTTP URL
- If the CRL file is not available in the CRL directory (or expired), and if the file cannot be downloaded from the CRL distribution point URL

Customizable properties

There are few CRL properties that can be configured through the `globalsettings.properties` file present under HP SIM's `\config` directory. The CRL GUI or the command line might not support all these settings.

- Download timeout of CRL file:
Property name: `CRL_FETCH_TIMEOUT`
The default value is 10000 (10s)
- The expiring delay is 1 day by default. This can be customized using:
Property name: `CRLExpirationStart`
The default value is 1
- If you do not want to receive alerts on CRL expiration:
Property name: `CRLAlert`
1 — Enable
0 — Disable
- Proxy settings:
The proxy host and port can be configured using the below properties. The proxy settings can be cleared off or removed if both these properties are removed, or set as empty in the `globalsettings.properties` file.
Property name: `PROXYHOST`
Property name: `PROXYPORT`

Certificate sharing

HP SIM supports a mechanism whereby other components installed on the system can use the same certificate and private key, facilitating authentication of the system as a whole instead of each individual component. This is currently used by the Web Agents and the WBEM components on the CMS.

SSH keys

An SSH key-pair is generated during initial configuration. The CMS public key is copied to the managed system using the `mxagentconfig` tool. This key-pair is not the same as for SSL and requires a manual process to regenerate a new pair. See the manpages or online documentation for `mxagentconfig` for more details. See the *Secure Shell (SSH) in HP SIM* white paper located at <http://www.hp.com/go/insightmanagement/sim/docs>.

The SSH keys of the trusted systems do not expire. These keys can be removed manually from the trust store.

Passwords

Passwords configured on the HP SIM **System Credentials** and **Global Credentials** pages are stored in the database encrypted using 128-bit Blowfish. These passwords can be further managed using the CLI command `mxnodesecurity`. A few passwords might be stored in a file on the CMS that are also encrypted using the same 128-bit Blowfish key. These passwords can be managed using the `mxcpassword` command. The password file and the Blowfish key file are restricted with operating system file permissions to administrators or root.

Prior to HP SIM 5.3, passwords configured on the HP SIM protocol settings pages are stored in a local file on the CMS, restricted with operating system file permissions to administrators or root. These passwords can be further managed using the `mxnodesecurity` command.

For User accounts, HP SIM relies on the customer environment (for example, Windows Operating System) to govern credential policy (expiration, logout, and so on).

Insight Control for VMware vCenter Server server authorizations

To register the Insight Control for VMware vCenter Server, discover the Insight Control for VMware vCenter Server itself, and then that discovery must include the UUID of the Insight Control for VMware vCenter Server.

- These credentials are typically set in discover task-specific credentials but can be system-specific or global.
- This does not have to be the same account that has access to Insight Control for VMware vCenter Server resources but it could be
- By default, to connect to WMI, Windows requires local admin access on the server (this is configurable on the Insight Control for VMware vCenter Server)
- Firewalls can block SNMP or WMI queries
- UAC can prevent even administrator credentials from running WMI queries with administrator privileges
- SNMP does not require any credentials but the SNMP service security must allow packets from the CMS
- SNMP or WMI is sufficient. If both are available a more complete description of the server is collected.

To communicate through Insight Control for VMware vCenter Server, proper permissions in vCenter access appropriate resources.

- vCenter uses Windows authentication and accounts
- This account does not require access to all ESX resources, only those to be managed by your Matrix
- It is stored on a separate page in HP SIM, Insight Control for VMware vCenter Server settings and may or may not match the server discovery credentials
- Typically access is granted to one or more "datacenter". Other resource collections also work, such as cluster.

NOTE: If the Insight Control for VMware vCenter Server is a VM guest, it is not required to discover its host. You can ignore warnings associated with an undiscovered host.

We require communications with WMI and/or SNMP.

For SNMP, a read community string must be known to the CMS. If SNMP packets are restricted to specific hosts, the CMS must be included in that list of hosts. No further credentials are required.

For WMI, the default Windows server install requires a local administrator account. However, this can be configured to allow access from any specific account.

Browser

SSL

All communication between the browser and the CMS or any managed server occurs using HTTPS over SSL. Any navigation using HTTP (not using SSL) is automatically redirected to HTTPS.

Cookies

Although cookies are required to maintain a logged in session, only a session identifier is maintained in the cookie. No confidential information is in the cookie. The cookie is marked as secure, so it is only transmitted over SSL.

A strict separation between the content provided by unrelated sites must be maintained on the client side to prevent the loss of data confidentiality or integrity. HP recommends you avoid links or resources that have arrived from unauthorized sites when a valid HP SIM session is running on browsers.

Passwords

Password fields displayed by HP SIM do not display the password. Passwords between the browser and the CMS are transmitted over SSL.

Password warnings

There are several types of warnings that can be displayed by the browser or by the Java plug-in on the browser, most having to do with the SSL server certificate.

- **Untrusted system**
This warning indicates the certificate was issued by an untrusted system. Since certificates are by default self-signed, this is likely if you have not already imported the certificate into your browser. In the case of CA-signed certificates, the signing root certificate must be imported. The certificate can be imported before browsing if you have obtained the certificate by some other secure method. The certificate can also be imported when you get the warning, but is susceptible to [spoofing](#) since the host system is not authenticated. Do this if you can independently confirm the authenticity of the certificate or you are comfortable that the system has not been compromised.
- **Invalid certificate>**
If the certificate is invalid because it is not yet valid or it has expired, it could be a date or time problem, which could be resolved by correcting the system's date and time. If the certificate is invalid for some other reason, it might need to be regenerated.
- **Host name mismatch>**
If the name in the certificate does not match the name in the browser, you might get this warning. This can be resolved by browsing using the system's name as it appears in the certificate, for example, `marketing1.ca.hp.com` or `marketing1`. The HP SIM certificate supports multiple names to help alleviate this problem. See the [“System link format” \(page 107\)](#) section below for information on changing the format of names created in links by HP SIM.
- **Signed applet**
Previous versions of HP SIM use a Java plug-in that can additionally display a warning about trusting a signed applet. Those previous versions of HP SIM use an applet signed by Hewlett-Packard Company, whose certificate is signed by Verisign.

Browser session

By default, HP SIM does not time-out a user session while the browser is displaying the HP SIM banner. This is known as monitor mode, and allows a continuous monitoring of the managed systems without any user interaction. The session times-out after 20 minutes if the browser is closed or navigates to another site.

An active mode is also supported where the session times out after 20 minutes if the user does not interact with HP SIM, by clicking a menu item, link or button. You can enable active mode by editing the `globalsettings.props` file and change the `EnableSessionKeepAlive` setting to `false`.

Best security practices include care when visiting other websites. You should use a new browser window when accessing other sites; when you are finished using HP SIM you should both sign out and close the browser window.

Internet Explorer zones

Internet Explorer supports several zones that can each be configured with different security settings. The name used to browse to HP SIM or managed systems can affect which browser zone Internet Explorer places the system. For example, browsing by IP address or full Domain Name System (DNS) (for example, `hpsim.mycorp.com`) can place the system into the browser's more restrictive Internet zone, causing improper operation. Ensure systems are being placed into the correct Internet zone when browsing. You might need to configure Internet Explorer, or use a different name format when browsing.

System link format

To facilitate navigation to managed systems, HP SIM provides the System Link Configuration option to configure how links to managed systems are formed. Go to **Options→Security→System Link Configuration**.

The following options are available:

- Use the system name
- Use the system IP address
- Use the system full DNS name

If you need full DNS names to resolve the system on your network, keep in mind that the browser might display a warning if the name in the system's certificate does not match the name in the browser.

Operating-system dependencies

User accounts and authentication

HP SIM accounts are authenticated against the CMS host operating system. Any operating system features that affect user authentication affect signing into HP SIM. The operating system of the CMS can implement a lock-out policy to disable an account after a specified number of invalid sign in attempts. Additionally, an account can be manually disabled in the Microsoft Windows domain. Any account that cannot authenticate against the operating system prevents signing into HP SIM using that account. For automatic sign-in to HP SIM, [user accounts](#) must be domain accounts.

NOTE: A user who is already signed into HP SIM is not re-authenticated against the operating system until the next sign in attempt and continues to remain signed into HP SIM, retaining all rights and privileges therein, until signing out of HP SIM.

-
- ❗ **IMPORTANT:** If creating operating system accounts exclusively for HP SIM accounts, give users the most limited set of operating system privileges required. Any root or administrator accounts should be properly guarded. Configure any password restrictions, lock-out policies, and so on, in the operating system.
-

File system

Access to the file system should be restricted to protect the object code of HP SIM. Inadvertent modifications to the object code can adversely affect the operation of HP SIM. Malicious modification can allow for covert attacks, such as capturing sign in credentials or modifying commands to managed systems. Read-level access to the file system should also be controlled to protect sensitive data such as private keys and passwords, which are stored in a recoverable format on the file system. HP SIM does not store user account passwords for users signing into HP SIM.

-
- ❗ **IMPORTANT:** HP SIM sets appropriate restrictions on the application files. These restrictions should not be changed because this could affect the operation of HP SIM or allow unintended access to the files.
-

Background processes

On Windows, HP SIM is installed and runs as a Windows service. The service account requires administrator privileges on the CMS and the database, and can be either a local or a domain account. For automatic sign-in to HP SIM, a domain account must be used. On UNIX, HP SIM is installed and runs as daemons running as root.

Windows Cygwin

The version of [Cygwin](#) provided with the [SSH server](#) for Windows, for CMS and the managed systems, has been modified with security enhancements to restrict access to the shared memory segment. As a result, it does not interoperate with the generally available version of Cygwin. Only administrative users can connect to a system running the modified SSH server.

HP-UX and Linux

The `device /dev/random` command is used, if available on the CMS, as a source for random numbers within HP SIM.

HP SIM database

Access to the database server should be restricted to protect HP SIM data. Specify appropriate non-blank passwords for all database accounts, including the system administrator (sa) account for SQL Server. Changes to the operating data, such as authorizations, tasks, and collection information, can affect the operation of HP SIM. System data contains detailed information about the managed systems, some of which might be considered restricted including asset information, configuration, and so on. Task data might contain extremely sensitive data, such as user names and passwords.

Configuring the SQL Server to enable SSL connection on database in HP SIM

To enable SSL DB communication in HP SIM, you must complete the following:

- [“Installing a certificate on a server with Microsoft Management Consold \(MMC\)”](#) (page 109)
- [“Configuring SSL for SQL Server”](#) (page 109)
- [“Configuration of client to enable trust”](#) (page 110)
- [“HP SIM database property settings to enable SSL for SQL Server”](#) (page 110)

Installing a certificate on a server with Microsoft Management Consold (MMC)

To use SSL encryption, you must install a certificate on the server where SQL Server is running. Complete the following steps to install the certificate by using the MMC snap-in.

Procedure 24 Configuring the MMC Snap-in

1. Open the certificates snap-in:
 - a. Open the MMC console by clicking **Start→Run**. The **Run** window opens.
 - b. Enter **MMC**.
 - c. From the **Console** menu, select **Add/Remove Snap-in**.
 - d. Click **Add**, and then click **Certificates**.
 - e. Click **Add**. You will be prompted to open the snap-in for the current user account, the service account, or for the computer account.
 - f. Select **Computer Account**.
 - g. Select **Local computer**, and then click **Finish**.
 - h. In the **Add Standalone Snap-in** box, click **Close**.
 - i. In the **Add/Remove Snap-in** bx, click **OK**. Your installed certificates are located in the **Certificates** folder in the **Personal** folder.
2. Install the certificate on the server using the MMC snap-in.
 - a. If you want to enable encryption for a specific client or clients, skip this step and proceed to ["Configuring SSL for SQL Server" \(page 109\)](#).
 - b. Select the **Personal** folder in the left-hand pane.
 - c. Right-click the right-hand pane, point to **All Tasks**, and then click **Request New Certificate**. The **Certificate Request Wizard** window opens.
 - d. Click **Next**.
 - e. Select **Certificate type is "computer"**.
 - f. In the **Friendly Name** text box, enter a friendly name for the certificate, or leave the box blank, and then complete the wizard. After the wizard completes, you will see the certificate in the folder with the fully qualified computer domain name.

Configuring SSL for SQL Server

Procedure 25 Configuring SSL for SQL Server

1. Configure SSL:
 - a. In the **Microsoft SQL Server** program group, click **Start**, and to **Configuration Tools**.
 - b. Click **SQL Server Configuration Manager**.
 - c. Expand **SQL Server Network Configuration**, right-click the **protocols for the server** you want, and then click **Properties**.
 - d. On the **Flags** tab, view or specify the protocol encryption option. The login packet will always be encrypted.
 - When the **ForceEncryption** option for the Database Engine is set to **Yes**, all client/server communication is encrypted and clients that cannot support encryption are denied access.
 - When the **ForceEncryption** option for the Database Engine is set to **No**, encryption can be requested by the client application, but is not required.
 - SQL Server must be restarted after you change the **ForceEncryption** setting.

2. Certificate requirement:

For SQL Server to load an SSL certificate, the certificate must meet the following conditions:

- a. The certificate must be in either the local computer certificate store or the current user's certificate store.
- b. The current system time must be after the **Valid from** property of the certificate and before the **Valid to** property of the certificate.
- c. The certificate must be meant for server authentication. This requires the **Enable Key Usage** property of the certificate to specify **Server Authentication (1.3.6.1.5.5.7.3.1)**.
- d. The **Subject** property of the certificate must indicate that the common name (CN) is the same as the host name of fully qualified domain name (FQDN) of the server computer. If SQL Server is running on a failover cluster, the CN must match the host name of FQDN of the virtual server and the certificates must be provisioned on all systems in the failover cluster.
- e. SQL Server 2008 R2 and the SQL Server 2008 R2 Native Client support wildcard certificates. Other clients might not support wildcard certificates. For more information, see the client documentation and Microsoft Knowledge Base KB258858 at <http://support.microsoft.com/kb/258858>.

Configuration of client to enable trust

Procedure 26 How to enable client to trust SSL connection

1. Export the certificates (chain) of SQL Server using MMC into files. Export the certificates in the following order: rootCA, intermediateCA, and server certificate.
2. Create a keystore on client-side using Java keytool or use JRE's keystore (cacerts).
3. Import the certificates into the keystore as trusted certificates in the following order:
 - a. Root certificate (root CA)
 - b. Intermediate certificate (intermediate CA)
 - c. Server certificate

How to test your client connection

Procedure 27 How to test your client connection

- To test your client connection, you can either:
 - a. Use the Query Analyzer Toolor
 - b. Use any JDBC/ODBC application where you can change the connection string.

HP SIM database property settings to enable SSL for SQL Server

To configure HP SIM to support SSL communication for SQL Server, complete the following:

Procedure 28 Configuring HP SIM property settings to enable SSL for SQL Server

1. Import the SQL Server certificates to `~/HP Systems Insight Manager/config/certstor/hp.keystore` as trusted certificates in the following order:
 - a. Root certificate (root CA)
 - b. Intermediate certificate (intermediate CA)
 - c. Server certificate
2. Change the following parameters in the `database.props` file:
 - a. `hp.Database.ssl=authenticate`
 - b. `hp.Database.username=username`
 - c. `hp.Database.password=password`
3. Change the following parameters in the `database.admin` file:

- a. `hp.Database.ssl=authenticate`
 - b. `hp.Database.username=username`
 - c. `hp.Database.password=password`
4. Append the following value at the end of the value set in the **connection-url** tab of the `hpsim-ds.xml` file, located in the `~/HP Systems Insight Manager/ jboss/server/hpsim/deploy/` folder.
`;ssl=authenticate`
 5. Restart the SQL Server services.
 6. Start HP SIM.

NOTE: This feature is supported only on Windows CMS with MS SQL Server as database. You can use Java keytool to import SQL Server certificate into the `hp.keystore` file. You can use HP SIM GUI by selecting tools.

For additional information, see:

<http://support.microsoft.com/kb/316898>

<http://msdn.microsoft.com/en-us/library/ms189067.aspx>

<http://msdn.microsoft.com/en-us/library/ms378567%28v=sql.90%29.aspx>

SQL Server and MSDE

HP SIM uses only Windows authentication with SQL Server and MSDE. The installation of MSDE with previous versions of HP SIM creates a random password for the sa account, though it is not used for HP SIM.

Remote SQL Server

SQL Server supports advanced security features, including SSL encryption during sign in and data communication. More information can be found in SQL Server documentation and the Microsoft website.

PostgreSQL

PostgreSQL uses a password that is randomly generated when HP SIM is installed. This password can be changed through the command line. See the `mxcpassword` manpage for more information.

Oracle

The Oracle database administrator must create a user (preferably with a non-blank password) for HP SIM to use when connecting to Oracle. The Oracle user must have, at the minimum, the Connect and DBA roles, which allow HP SIM to have the correct privileges to create and delete HP SIM tables and views, along with read/write access to the HP SIM tables. Changes to the operating data, such as authorizations, tasks, and collection information, can affect the operation of HP SIM. System data contains detailed information about the managed systems, some of which might be considered restricted, including asset information, configuration, and so on. Task data can contain extremely sensitive data, such as user names and passwords.

Command-line interface

Much of HP SIM's functionality can be accessed through the command line. To access the command-line interface, you must be logged on to the CMS using an operating system account that is a valid HP SIM user account. That account's authorizations and privileges within HP SIM apply to the command line interface as well.

NOTE: On a Windows system, the operating system account must have administrator-level access on the CMS for all of the commands to work properly.

How to: configuration checklist

General

- Access to the CMS must be restricted, both at the network operating system-level and at the physical-level.
- A strict separation between the contents provided by unrelated sites must be maintained on the client side to prevent the loss of data confidentiality or integrity. HP recommends you avoid links or resources that have arrived from unauthorized sites when a valid HP SIM session is running on browsers.
- Configure firewalls to allow desired ports and protocols
- Review lockdown versus ease of use
- After configuring the CMS and managed systems, run discovery on the CMS
- User account policies (password, lockout, and so on) must be configured and enforced by your environment.
- CMS must be configured on the local intranet.

Configuring the CMS

- Inspect SSL server certificate and update if desired
- Configure passwords and SNMP community strings (See the [“Configuring managed systems”](#) (page 112) section below)
- Configure user accounts, based on operating system accounts that will access HP SIM
- Review and configure toolboxes if defaults are not appropriate
- Review and configure authorizations for users
- Configure system link configuration format
- Review audit log

Strong security

NOTE: How-to: lockdown versus ease of use for more details.

- Enable **Require Trusted Certificates**, inspect and import desired system SSL certificates or root signing certificates
- Require only known SSH keys, inspect and import desired system SSH public keys

Configuring managed systems

- Configure SNMP community strings, which are required at the CMS.
- For WBEM on HP-UX and Linux, configure the WBEM password. This password is required at the CMS. For the highest level of security, a different user name and password can be used for each managed system; each user name and password pair must be entered into the CMS to enable access.

For HP-UX, certificates can be used instead of username and password for WBEM authentication. For more information, see the HP SIM online help.

- The CMS requires a user name and password to access WMI data on Windows systems. By default, a domain administrator account can be used for this, but you should use an account with limited privileges for WMI access. You can configure the accounts accepted by each Windows managed system by using the Computer Management tool:
 1. Select the **WMI Control** item.
 2. Right-click **WMI Control**, and then select **Security**.
 3. Select the **Security** tab, select **Root namespace**, and then click **Security>**
 4. Add a user to access WMI data along with their access rights. The **enable account** and **remote enable permissions** options must be enabled for correct operation of HP SIM.
 5. The user name and password specified here must be configured in the CMS.
- Set up user accounts for Insight Web Agents
- Add the CMS SSH public key to the system's trusted key store by running `mxagentconfig` on the CMS.
- Configure trust relationship option for Insight Web Agents; import the CMS SSL certificate if set to trust by certificate.

⚠ CAUTION: Establishing the trust by certificate for HP SMH enables any HP SIM user to gain administrative access to the HP SMH hosts. This enables the HP SIM user to execute any command remotely on the HP SMH host.

How to: lockdown versus ease of use on Windows systems

Moderate

The HP Insight Management Agents should be configured to trust by certificate. This requires distributing the HP SIM certificate, which includes the public key, to all the managed systems. After the systems have been configured to trust the HP SIM system, they will accept secure commands from that particular system only.

This certificate can be distributed in a number of different ways, including:

- Use the Configure or Repair Agents **Set Trust Relationship** option in HP SIM to deploy the HP SIM certificate to the managed systems. Depending on the managed system, this might use SSL or Windows network connections to copy files and configure the managed systems.
- Use the Web-based interface in an individual Insight Management Agent to specify the HP SIM system to trust. This causes the agents to pull the digital certificate from the HP SIM system immediately, enables you to verify it, and then sets up the trust relationship. While this option does have some limited vulnerability, it would be possible to spoof the HP SIM system at the time the certificate is pulled and thus set up an unexpected trust relationship. However, it is reasonably secure for most networks.
- Import the HP SIM certificate during initial installation of the Insight Management Agents. This can be done manually during an attended installation or through the configuration file in an unattended one. This method is more secure because there is little opportunity for the spoofing attack described above.
- If you have already deployed the Insight Management Agent, you can distribute the security settings file and the HP SIM certificate directly to the managed systems using operating system security.

- ❗ **IMPORTANT:** When using the **Trust by certificate** option, the HP SIM SSL certificate must be redistributed if a new SSL certificate is generated for HP SIM. SSH on the managed system normally operates in a mode similar to trust by certificate in that it requires the SSH public key from the CMS. Note that the SSH public key is not the same as the SSL certificate. The command `mxagentconfig` is used on the CMS to copy the key to the managed system. This must be done for each user account that is to be used on the managed system since the root or Administrator account is used by default.

The HP SIM SSH public key must be redistributed if the SSH key-pair is regenerated.

Strong

The strong security option lets you take advantage of every security feature. This option provides the highest level of security available within the HP SIM security framework, but there are some additional procedural steps you must make in your server operations. Also, this option is facilitated by using your own PKI that includes a certificate authority and certificate server.

Procedure 29 Setting security to strong

1. Generate certificates from your certificate server for each managed system and the HP SIM system. To do this, first generate a certificate signing request (CSR) from the various systems. This generates a PKCS#7 file. This file should then be taken to the certificate server and signed, and then the resulting file (generally a PKCS#10 response) should be imported into the each managed system and the HP SIM system.

To maximize security, it is important that none of these steps be done over a network unless all communications are already protected by some other mechanism.

Thus, in the case of the Insight Management Agent, a removable media (for example, USB thumb drive, floppy disk) should be taken directly to the managed system, have the PKCS#7 file placed on it, and hand-carried to a secure system with access to the certificate server. The PKCS#10 response file should similarly be placed on the removable media and returned to the managed system to be imported into the Insight Management Agent.

2. Take the root certificate (just the certificate, not the private key) of your certificate server and import that into the HP SIM trusted certificate list. This allows HP SIM to trust all the managed systems because they were signed with this root certificate.
3. Take the certificate from the HP SIM system and import it into the Insight Management Agent of each system. This allows the managed systems to trust the HP SIM system. This certificate can be distributed using any of the methods available to distribute the HP SIM certificate. However, the option to pull the certificate directly from the HP SIM system over the network must be avoided due to the potential man-in-the-middle attack.

As in the Moderate option, you must redistribute the HP SIM SSL certificate to the managed systems whenever a new HP SIM SSL certificate is generated.

4. Once these steps have been completed, you can turn on the option in HP SIM to enable **Require Trusted Certificates**. Select **Options**→**Security**→**Trusted Systems**, and then click **Trusted Certificates**. The warnings presented around this option make it clear that any managed system that does not have a certificate signed by your certificate server will not be sent secure commands from the HP SIM system, although it will be monitored for hardware status.

5. For SSH, turn on the option to accept SSH connections only from specified systems. Select **Options→Security→Trusted Systems**, click **SSH Host Keys**, and then enable the **The central management server will accept an SSH connection only if the host key is in list below**. Afterwards, you must manually import each managed system's public SSH key into the list of keys in HP SIM.

To configure this in previous versions of HP SIM, add or modify the following line in the `Hmx.properties` file:

```
MX_SSH_ADD_UNKNOWN_HOSTS=false
```

and then restart HP SIM.

Afterwards, you must manually import each managed system's public SSH key into the list of keys in HP SIM.

21 Privilege elevation

Privilege elevation enables users without root privileges to run tools requiring root privileges on HP-UX, Linux, and VMware ESX managed systems. To use this feature with HP SIM, a privilege elevation utility such as `su`, `sudo`, or Powerbroker must be installed on the managed system. Typically, these utilities are used to sign in as a normal user, then when you want to run a program requiring root, prefix the command line for that program with the privilege elevation utility's executable. For example `sudo rm /private/var/db/.setupFile`. Some of these utilities can be configured to prompt the user for a password before allowing root access.

For HP SIM to run tools on managed systems using privilege elevation, HP SIM must be configured to know which user to use to sign in to the managed systems, how to prefix the command line that it will run, and whether or not the privilege elevation utility will prompt for a password. This is configured either from the First Time Wizard, or from the **Options** menu by selecting **Options**→**Security**→**Privilege Elevation**. You can configure different values of these settings for Unix and Linux systems versus VMware ESX systems.

- ❗ **IMPORTANT:** Whenever privilege elevation is enabled, the other tools, which make use of privilege elevation, must provide the privilege elevation password.

Once you have configured HP SIM to use privilege elevation, it determines if a tool needs privilege elevation by looking at the tool's `execute-as` parameter. This is the user the tool should be run as on the managed system. If this parameter is specified as `root` in the tool's tool definition file (`tdef`), then HP SIM will invoke privilege elevation. If this parameter is not specified in the `tdef`, then HP SIM defaults the value of `execute-as` to be the identity of the user invoking the tool within HP SIM. If this user is logged in as root, then privilege elevation will also be used.

When HP SIM determines that privilege elevation should be used, it uses SSH to sign in to the remote system with the user that was configured in the privilege elevation settings page (a specific user, the user who is currently signed into HP SIM, or a user specified at runtime). If the user must be specified at runtime, or if a password is required for privilege elevation, these prompts appear on the Task Wizard page that collects any parameters necessary to run a tool. After HP SIM is signed into the remote system through SSH, it invokes the command for the tool, prefixed by the privilege elevation utility executable, and supplies the password if required.

Two-factor authentication

The two-factor authentication is an alternative technique that an full rights user can configure as a logging mechanism for HP SIM. This signin technique offers a more secure communication than the user name and password technique, as it requires two factors to sign in to the system. The two factors are:

- Smartcard
- Personal Identification Number (PIN)

Two-factor authentication is applicable to HP SIM's web interface and is applicable to port 50000.

Enabling and disabling two-factor authentication

HP SIM uses user name and password mode of signin by default. The two-factor authentication technique can be enabled or disabled from the GUI by selecting **Options**→**Security**→**Two-factor Authentication**→**Change Authentication Mechanism**. The same can be configured through the command line interface:

```
mxauthnconfig -m 0|1
```

After enabling or disabling two-factor authentication, the HP SIM service must be restarted for the changes to take effect. Only one authentication technique will be enabled at a time. All users will be authenticated based on the currently enabled authentication technique.

Enable secure communication

HP SIM ensures that the user certificate contained in the smart card is trusted by a valid and known Certificate Authority (CA). It allows users to login to the CMS only if the certificate is trusted, and is not expired or revoked by the CA issuer, and also it ensures that the user is a valid SIM user.

Directory structure users

Two-factor authentication is not supported for local CMS users. It is supported for domain users which are configured in Microsoft Active Directory or any other directory service; for example, Apache directory, and so on. HP SIM expects one user account to be saved in HP SIM. This account can be configured from the GUI by selecting **Options→Security→Two-factor Authentication Configuration**, or by using the command line interface `mxauthnconfig -a`. Refer to *HP SIM Command Line Guide* for more information.

Users Distinguished Name

It is important to save the Users distinguished name (DN) in HP SIM where all the certificate based users are configured. HP SIM does not support multiple users distinguished names. User Name Attribute should be supplied with a field that is unique in directory structure and can be used to uniquely create a user in HP SIM. This can be `sAMAccountName` in the case of Active Directory, or any unique field, such as `UID/ID/email/emplD` in the case of open directories.

Subject Alternative Name

HP SIM expects all certificates to possess the Subject Alternative Name->Other name field which contains the User Principal Name. This User Principal Name will map user's account in HP SIM.

Authentication phase

This phase involves validating the certificate for the following requirements:

- If the certificate is trusted by a valid or known Certificate Authority (CA)
- If the certificate is not expired and is still valid.
- If the certificate is not revoked by the CA.

If any of these validations fail, an error will be reported to the user by the CMS.

Authorization phase

The authentication phase is followed by the authorization phase.

This phase involves authorizing the user to execute tasks in the CMS. This step verifies that the authenticated user has a valid HP SIM user account.

Certificate revocation check

This is one of the pre-requisites to enable two-factor authentication.

Pre-requisites to enable two-factor authentication technique

- A domain server account must be configured in HP SIM.
- The users distinguished name must be configured in HP SIM.
- The certificate revocation check must be configured in HP SIM. Please see "[Certificate expiration and Certificate Revocation Check \(CRL Check\)](#)" (page 102)) for more information.
- The root and intermediate CA certificates associated with the user certificates must be imported into HP SIM. This can be done by selecting **Options→Security→Credentials→Trusted Systems→Trusted Certificates**.
- Switch to two-factor authentication mode and restart CMS.

All users must possess certificates to login to HP SIM.

Administrators can still be able to access all CLIs (such as `mxuser`, `mxnode`, and so on) when HP SIM runs on two-factor authentication mode.

Smart cards and Cryptographic Service Provider (CSP)

HP SIM does not directly communicate with the Cryptographic Service provider rather it leverages the capabilities from the browser. It is expected that browsers need to be configured manually to communicate with the Smart card's CSP. Browsers must be able to recognize smart cards and prompt for PIN when user connects to HP SIM.

For instance, if Active Client is installed and running on a client workstation, and if user connects to HP SIM through Internet Explorer, then Internet Explorer will start communicating with the Active Client CSP and will prompt the user to insert the Smart card.

Security measures to follow

- You are advised to close the browser and remove the smart card immediately after you have logged out of HP SIM. This will clean up any certificate cached by the browser, or by the software CSP.
- It is recommended to use a fresh browser window to login to HP SIM.
- Always insert Smart card before connecting to HP SIM. Few browsers might not recognize or communicate with the CSP until you insert the smart card.
- Whenever you get any error during the course of authentication, close the browser and retry. This is because the browser will treat the current session as failed and will not allow you to re-handshake with the server.
- Do not store your certificates in the browser. This might enable others to use your certificate.

Login steps:

- Type `https://<CMS>:50000` from the browser (IE or firefox).
- If the browser is configured properly, you will be prompted to pass the PIN
- User is authenticated and authorized successfully.

22 HP SIM quiesce

HP SIM Quiesce is an independent entity which performs the operation of pausing and resuming the operations of HP SIM. It helps to allow in-progress tasks to complete and block new tasks from starting, so that a clean backup or export of the CMS management data can be taken.

The task criticality is used during the quiesce operation, which is part of Unattended Backup. When the system is quiesced, you cannot start any new tasks, or delete or modify existing tasks.

The two main operations of HP SIM Quiesce are:

- Quiesce
- Unquiesce

The expected behavior when HP SIM is quiesced is:

- Lock the system so that the state of the system is not changed, unless the unquiesce operation is executed.

Locking the system includes:

- Not allow any new tasks to be started, any existing tasks to be deleted or modified
- Not allow any CLI command that would modify the state of HP SIM to be executed
- Not allow any SOAP calls that would modify the state of HP SIM to be executed
- Any running tasks should either be killed or allowed to complete, depending on the criticality of the task.
 - Critical tasks are allowed to complete
 - Non-critical tasks are cancelled

The expected behavior when HP SIM is unquiesced, is to unlock the system so that you can proceed with normal operations

Whenever HP SIM is quiesced, you can see the state in the top banner of the HP SIM GUI.

See the *HP Systems Insight Manager Command Line Interface guide* at for additional information about setting task criticality using the command line. See the HP SIM online help to see how to set the criticality using the GUI.

23 Contract and warranty

The **Contract and Warranty Status** is available when you have a Windows CMS, and the HP Insight Remote Support Pack is installed. You can view Contract and Warranty status updates for HP systems that have contract and warranty data collection enabled. Click the **Contract and Warranty Status** icon to view the **Contract and Warranty Details** page for the system.

The following requirements must be met in order to view contract and warranty data in HP SIM:

- The HP SIM CMS must have connectivity to <http://www.hp.com>.
- The Remote Support Pack software must be installed and properly configured. The Remote Support Software Manager is installed on the CMS during the HP SIM installation. After the HP SIM installation is complete, you must configure the Remote Support Software Manager to fit your enterprise specifications. Once configured, the Remote Support Software Manager will download and install the Remote Support tool. The Remote Support tool must be installed, configured, and registered before you can retrieve contract and warranty data.
- To collect contract and warranty data for a system, the system's serial number, product ID, and country code must be present in the system properties. In most cases, the serial number and product ID are obtained during HP SIM's identification process. You can enter a serial number and product ID if needed. It is important to specify the correct country code to ensure accurate information. If HP SIM cannot obtain a country code, it defaults to *US*. If you have a support contract, enter an entitlement or obligation identifier and entitlement type if you want to view contract data.

NOTE: Collecting Contract and Warranty information is limited to once a day.

Viewing contract and warranty information

You can view contract and warranty information by:

- Clicking the **CW** icon in the system table view page.
- Clicking the **Contract and Warranty status** link on the system page.
- Viewing a **Warranty-Contract** report.
- Searching for systems with contracts or warranties that expire in a specified number of days.
- Configuring alerts for systems with expiring contracts or warranties.
- Viewing the initial and monthly contract and warranty data collection tasks.
- Viewing the **Remote Support Eligible** collection, which lists systems the Remote Support Pack supports if you choose to enable them for support and are entitled to support. If a system is enabled without proper entitlement, events are submitted to the Remote Support tool, but they are not monitored and will not trigger a response.

NOTE: If you receive an incorrect response for a particular HP brand system after clicking the **CW** icon on the system table view page, there might be an entitlement issue with the system. This is not a Remote Support or an HP SIM issue. Please contact HP support. You must have a valid serial number, product ID, and any contract or Care Pack numbers that are applicable.

Collecting contract and warranty data

The following tasks are used to collect contract and warranty data:

- **Initial contract and warranty collection.**

This task collects contract and warranty data from newly discovered systems. If the required system properties are not entered for a new system or automatically collected by HP SIM during identification, contract and warranty data will not be collected.

- **Monthly contract and warranty collection**

This task collects contract and warranty data every month. If the required system properties are not entered for a system or automatically collected by HP SIM during identification, contract and warranty data will not be collected.

If you want to run the Contract and Warranty Collection task immediately for an updated system, select **Options**→**Contract and Warranty Data Collection**. Collecting Contract and Warranty information is limited to once a day.

❗ **IMPORTANT:** Running the contract and warranty collection task more than once a month is not recommended or needed since the data does not often change.

Viewing contract and warranty status

Overview

The **Contract and Warranty Status** page is available when you click the **CW** icon on the system table view page or the **Contract and Warranty Status** link on the system page. This page lists **System Information** and contract and warranty details.

NOTE: A system can have multiple contracts and warranties.

System Information

- **System Name**

The system name or IP address.

- **Serial Number**

The system serial number. This can be the serial number discovered by HP SIM or the number you entered in the **Customer-Entered serial number** field on the **Edit System Properties page**.

- **Registered Product Number**

The product number. Typically, the product number is the number used to order a system.

- **Product Line**

Details about the product line.

Contract

- **CCRN (Customer Contract Reference Number).**

The reference used for the contract as renewed over time.

- **Active Contract**

This value is **true** if an active contract exists.

- **Start Date**

The start date of an active contract.

- **End Date**

The end date of an active contract. If no end date is available, this field is blank.

- **Contract Status**

The possible values are:

- A: Active
- F: The start date is in the future
- X: Expired
- E: There is no end date
- I: The agreement is informal. This status might mean that the agreement is not finalized.
- B: Delivery blocked
- C: Cancelled

- **Active Obligation**

This value is **true** if there is an active support contract for a system.

The contract start and end date is listed for each contract item along with the following information:

- **Status**

The possible values are:

- A: Active
- F: The start date is in the future
- X: Expired
- E: There is no end date
- I: The agreement is informal. This status might mean that the agreement is not finalized.
- B: Delivery blocked
- C: Cancelled

- **Service Level**

The level of service specified in the offer. This includes the amount of time HP has to react to an issue, the time to resolution for a set of issues, and the type of response HP will use to react to an issue.

- **Deliverables**

A description of services offered with this contract, for example, onsite support or parts and materials.

Warranty

- **Warranty Type**

The type of warranty, for example, Base Warranty, Bundled Warranty, or HP Care Pack.

- **Start Date**

The start date of an active warranty.

- **Extension**

The number of days that this warranty has been extended.

- **Wty: HP HW Maintenance Onsite Support**

The warranty start and end date is listed for each warranty item along with the following information:

- **Status**

The possible values are:

- A: Active
- F: The start date is in the future
- X: Expired
- E: There is no end date
- I: The agreement is informal. This status might mean that the agreement is not finalized.
- B: Delivery blocked
- C: Cancelled

- **Service Level**

The level of service specified in the warranty. This includes the amount of time HP has to react to an issue, the time to resolution for a set of issues, and the type of response HP will use to react to an issue.

- **Deliverables**

A description of services offered with this warranty, for example, onsite support or parts and materials.

- **Wty: HP Support for Initial Setup**

- **Status**

The possible values are:

- A: Active
- F: The start date is in the future
- X: Expired
- E: There is no end date
- I: The agreement is informal. This status might mean that the agreement is not finalized.
- B: Delivery blocked
- C: Cancelled

- **Service Level**

The level of service specified in the warranty. This includes the amount of time HP has to react to an issue, the time to resolution for a set of issues, and the type of response HP will use to react to an issue.

- **Deliverables**

A description of services offered with this warranty, for example, onsite support or parts and materials.

Monitoring contract and warranty status

Contract and warranty status is shown by the following status types:

Table 9 Contract and Warranty status

Status Icon	Icon Meaning	Description
	Major	The contract or warranty is expired
	Minor	- Contract information is temporarily unavailable. - The contract expires in 30 days.
	Warning	The contract expires in 90 days.
	Normal	The system has a valid contract or warranty.
	Unknown	No contract information was found. The system might not have a serial number or product ID.
	Disabled	The Do not collect contract and warranty data for this system option is set for the system.

24 License Manager

License Manager enables you to view and manage product licenses within the HP SIM user interface. To access additional information about Updates, Upgrades, and Technical support, contact your HP services or HP partner representative or access the HP Support Center at www.hp.com/go/hpsc.

NOTE: To run License Manager, you must have **administrative rights** on the CMS (to set, select **Options**→**Security**→**Users and Authorizations**→**User**) and choose the **Configure CMS Security** option, and the **All Tools** toolbox (to set, select **Options**→**Security**→**Users and Authorizations**→**Authorizations**) on the managed systems that you want to license.

You can view and associate licenses to specified target **systems** discovered by HP SIM. A product may use artificial systems to contain licenses. Therefore, you may see names of non-existent systems. System licenses can be reviewed by product. Licenses can be associated with specific systems. Licenses can be collected and deployed to management processors. New licenses can be added individually or in bulk from a file. License Manager database tables are updated and synchronized daily at midnight or at HP SIM startup, and expired license information is sent to registered plug-ins.

For some products, License Manager only permits users to review system licenses, available licenses, and add licenses. For other products, License Manager allows association of licenses with systems selected by the user. The association of the license is dependent on the particular product. For some products, licenses can be freely associated with selected systems and those associations can be changed. However, in most cases the license is locked to the system once it is used with the product. Once locked, associations can no longer be changed. For other products, the product association is permanent once made in License Manager. Finally, some products allow License Manager to manage their licenses entirely such that selection and licensing systems is final. The distinction between these latter modes is that associations may be changed if the user options include Assign / Un assign and are final if there is one option, Apply.

License Manager includes functionality to collect and deploy licenses with most management processors. The License Manager core establishes and maintains a secure communication channel for license deployment with the management processor through two options provided by HP SIM, SSL and Secure Shell (SSH). Both, SSL and SSH meet the requirements for a secure channel. If the target systems are management processors, the management processor must support SSH and you must provide the required credentials. An SSH based solution uses CLO. All management processor firmware releases include support for SSH/CLP. ProLiant SSH/CLP support is included in v1.70 or later of the management processor firmware. Integrity SSH/CLP support is included in management processor firmware. All management processors can be updated to this version or later. The license collection uses an HTTP based mechanism and operates without credentials. Management processor firmware in many instances allows the user to define if license information is available on demand using this mechanism.

Table 10 Supported hardware for Integrity management processor license collections

Hardware	Product name	Server type	Firmware support
rx2660	Merlin	Rack	F.02.19 or greater
rx3600	Ruby	Rack	F.02.19 or greater
rx6600	Sapphire	Rack	F.02.19 or greater
BL860c	Tahiti	Blade	T.03.07 or greater
BL870c	Barbara	Blade	T.03.07 or greater

NOTE: The new management processor license collection is supported on management processor and management processor devices. Deployment is supported on management processor and management processors with newer firmware versions.

In some instances, licenses are managed and controlled by the licensed system (remote licensing). In this case, License Manager provides the facility to collect and deploy licenses to those systems. For non-management processor systems, communication used is a Microsoft COM mechanism.

For some products, the license is stored in a licensing structure in the Windows registry on the licensed system. License Manager employs Microsoft's remote registry API over the COM protocol to assign licenses to and collect license information from those remote systems. License information is duplicated in the HP SIM database, but licenses are managed remotely and must be periodically collected to keep this information correct. Authentication credentials for the specified systems are needed when licenses are sent to the specified system. If WBEM authentication credentials have been provided for a specific target, these credentials are used. If specific credentials have not been provided, each set of WBEM credentials provided as global credentials are used in turn. If no credentials are provided, the connection is attempted using the default credentials of the HP SIM server. The remote registry service must be started and run on candidate target systems for key collection or assignment. This mechanism of license management is rare. Those instances where used, will be clearly stated in product documentation.

NOTE: Automatic collection of management processor licenses is not supported.

NOTE: You do not have support or upgrade options by default. After July 9, 2007, all license keys are included in one year of 24 x 7 Software Technical Support and Update Service. The License Manager informs you which license keys are "support and update enabled" and which license keys require the purchase of future updates and upgrades.

CLI mxlmkeyconfig

The CLI `mxlmkeyconfig` enables you to combine all the License Manager key files into one file instead of having to execute multiple files. Combining these files into a single file makes it easier when adding keys from a file through the License Manager graphical user interface.

The `mxlmkeyconfig` command takes all the keys and related information and places it in the resulting key file. The CLI program will not allow duplicates. If there are duplicate <key string> values, a warning message appears and only the first value is placed in the resulting key file. If badly formatted files are encountered, warning messages appear.

The key file is created when the CLI `mxlmkeyconfig` command is executed. If the resulting key file already exists, then the previous keys remain and the information from the source key files are added to the resulting key file.

License types

License Manager displays licenses by product. If a license authorizes multiple products, the number of seats permitted by the license is applied in full to each authorized product. For example, a license authorizing five seats and two products authorize five seats for each product.

Table 11 License types

License Type	Description
Flexible Quantity	Offers full, unlimited functionality for an unlimited time and for a specific number of seats purchased, up to 50,000.
Activation Key Agreement	Offers full, unlimited functionality for an unlimited time. This license represents an expected upper limit on the number of seats, up to 50,000.

Table 11 License types *(continued)*

License Type	Description
Demo (seats and time)	Offers full, unlimited functionality for a limited time and a specific number of seats. The license determines the number of days the key enables the product to function. The days begin counting from the day of first use. The key can permit more than one instance of the product to run. Demo keys can authorize up to 255 seats for up to 255 days.
Demo (time)	Offers full, unlimited functionality for a limited time. The license determines the number of days the key allows the product to function. The days begin counting from the day of first use. The key can permit more than one instance of the product to run. Demo keys can authorize use for up to 65,535 days.
Beta	Offers full, unlimited functionality for a limited time. The license determines the number of days the key enables the product to function. The days begin counting from the day the key is created. The key can permit more than one instance of the product to run. Demo keys can authorize use for up to 65,535 days.
Duration	Offers time limited, full functionality license. A Duration license (DLL) can be assigned to a system multiple times. When the licensed product consumes a license and that license subsequently expires, a new license will be consumed and removed from the stack of assigned licenses (if there are any and using the same license key). For example, if seven product licenses from the same DLL key are assigned the license remains valid for seven times the interval specified in the corresponding DLL license. Any number of the assigned licenses still assigned can be unassigned at any time.. The basic time unit encoded in the key is one month. A DLL can authorize up to 255 seats for up to 255 months.
Subscription	Offers time limited, full functionality license. The basic time unit encoded in the key is one month. A Subscription license can authorize up to 255 seats for up to 255 months. All subscriptions licenses based on a specific subscription license key will all expire when the first license used from this key expires. All time representations in License Manager displays are in days

NOTE: HP SIM considers one month equal to 30 days.

Table 12 License types reported by management processor products

License Type	Description
Intrinsic	Offers full, unlimited functionality and represents a single-use key for the product. This license type is specific to management processors.
Individual	Offers full, unlimited functionality and represents a single-use key for the product. This license type is specific to management processors.
Permanent	Offers full, unlimited functionality.
Demo (time)	Offers full, unlimited functionality for a limited time. The license determines the number of days the key allows the product to function. The days begin counting from the day of first use. The key can permit more than one instance of

Table 12 License types reported by management processor products *(continued)*

License Type	Description
	the product to run. Demo keys can authorize use for up to 65,535 days.

Licensed System(s)

License Systems in License Manager enables you to list the systems licensed for the selected product. Products can elect to not display all or some licensing details.

Some products provide licenses to enable other products. The license keys generated by these products can be manually added. In many instances, these generated licenses are not visible to the user. Therefore, the only way to determine if a system is licensed for a product is to check the license status of the enabling product and noting this relationship.

Add Licenses

HP SIM enables you to add individual license keys to the License Manager database.

HP iLO product license keys can be added into the database because they can be deployed directly to management processors.

Collect Remote License Info

Collect Remote License Info (for management processors) collects licenses using an HTTP based protocol which does not require credentials.

When collecting remote licenses, be aware of the following:

- Automatic collection of management processor licenses is not supported.
- You do not have support or upgrade options by default. After July 9, 2007, all license keys are included in one year of 24 x 7 Software Technical Support and Update Service. The License Manager informs you which license keys are "support and update enabled" and which license keys require the purchase of future updates and upgrades.

Collect Remote License Info (for servers) collects license details from selected targets. If licenses are stored on the selected system (for details, see the specific product information), the selected machine must be running a variant of Microsoft Windows.

This collection process will do the correct behavior when a product has been selected in Product License Information table above. When no product has been selected, the behavior is determined by the type of system selected. When no product has been selected, select the management processor and NOT the server hosting the desired management processor.

License Collection Results table

Collect Remote License Info			
License Collection Results			
System Name	Key	Product	Response Status
15.154.109.180			This target system does not support the selected product.
15.154.109.181			This target system does not support the selected product.
15.154.109.182	323K3-78P34-MCLDQ-LPY2N-TSHSR	ILO Advanced	Licensing information from the remote system.
15.154.109.183			This target system does not support the selected product.
15.154.109.185	323K3-78P34-MCLDQ-LPY2N-TSHSR	ILO Advanced	Licensing information from the remote system.
15.154.109.186			This target system does not support the selected product.
15.154.109.187	323K3-78P34-MCLDQ-LPY2N-TSHSR	ILO Advanced	Licensing information from the remote system.
15.154.109.188			This target system does not support the selected product.
15.154.109.189			This target system does not support the selected product.
15.154.109.190			This target system does not support the selected product.
15.154.109.192			This target system does not support the selected product.
15.154.111.24			This target system does not support the selected product.
15.154.126.146	323K3-78P34-MCLDQ-LPY2N-TSHSR	ILO Advanced	Licensing information from the remote system.
15.154.126.208			This target system does not support the selected product.
15.154.126.209			This target system does not support the selected product.

1 System Name. The names of the systems where the task was executed.

- 2 **Key.** The license keys received from the target systems. Each key retrieved from a system is on a separate line. Some products have more than one license key. License details are contained in the key, and each key might enable more than one product.
- 3 **Product.** The name of the product associated with the use of this key.
- 4 **Response Status.** The status of the request for license data for the selected system.

- Successful task
 - A. Licensing information from the remote system.
 - B. Licensing information from the target system.

NOTE: This response status displays for systems running Windows variant OS and has license stored in the registry.

- Unsuccessful task
 - A. Connection to device failed. Possible reasons could be device not reachable or device is an older firmware version of management processor.
This happens due to the following reasons:
 - a. Network error - Connection Refused.
 - b. Network error - Connection timed out.
 - c. The system you are trying to connect has firmware version that is older or not supported.
 - B. Device not found.
Failure in pinging the system.
 - C. License Key overused. Please refer to the license agreement to avoid any violations.
 - D. No valid licensing information found on the remote system.
 - E. No licensing information on the remote system.
 - F. Problem collecting licensing information.
 - G. Failed to contact this system. Network path not found or similar error.
 - H. Specified system is no longer in the database.
 - I. Target system is not running Microsoft Windows as required.
 - J. Keys cannot be collected from a system of this type.

NOTE: This displays if the system is of a different type such as; a switch, a printer, a cluster, a complex, or a system not running a Windows OS.

- K. Cannot collect keys stored on this node. HP SIM host and specified system must be running Microsoft Windows.

NOTE: This happens when, for example CMS or a remote system is not running a Windows variant operating system.

- L. License Manager does not know how to assign licenses for this product. License Manager has no information about this product. Install the HP Systems Insight Manager plug-in that uses this license or collect license information from a system running this product first.

Assigning and Unassigning licenses

HP SIM enables you to assign and Un assign product licenses for plug-ins, if applicable for that plug-in, and to assign licenses to remote target systems when licenses are managed remotely. Remember that management processor licenses must be applied directly to the management processor and NOT its host server. For plug-ins, when assigning licenses, note the following for non-management processor targets:

- When a license is assigned to a system, it is not locked or consumed until the product operates on that system.
- A system can be licensed with a demo key just once. If the license expires, the only option to continue to use the system with that product is to purchase a license. A system licensed by a demo key can be relicensed at any time with a paid license.
- An assigned license can be unassigned from one system and assigned to another system, as long as the product enabled by the license has not consumed the license. When a product has been used on a system, the license is locked to that system permanently. Licenses delivered directly to a target system that manages its own licenses cannot be unassigned (product will provide details on when a license must be sent to a remote server). There is no penalty for having these licenses remain on those systems because they are consumed on an as-needed basis. The remaining licenses can be used elsewhere.
- A DLL can be assigned to a system a multiple number of times. When the licensed product consumes a license and that license subsequently expires, a new license will be consumed and removed from the stack of assigned licenses (if there are any and using the same license key). For example, if seven product licenses based on the same DLL key are assigned, the license remains valid for seven times the time interval specified in the corresponding DLL license. Any number of the assigned licenses still assigned may be unassigned at any time.

Some products limit the use of the License Manager interface. Consequently, **Manage Licenses** may be selected, however **Apply** or **Assign/Un-assign** might be disabled.

Apply Licenses

A license applied to a system is irreversible. Licenses applied to management processors are managed by each management processor and so the policy is set by the management processor. The license is locked to the specified system.

For management processor targets:

- When a license is assigned to a management processor, a license record is created and stored in the License Manager database.
- If the selected management processor is already licensed, you cannot replace that license with a new license from License Manager. You must first delete the existing license at the management processor console and then insert the new license (directly or using License Manager). However, Integrity MP does replace a demo key with a permanent license. If a permanent key is already present, Integrity MP displays a message such as `License already Installed`.
- An assigned license cannot be unassigned from one management processor and assigned to another management processor. Licenses delivered directly to the actual target system cannot be unassigned because the behavior of the product operating with that license is outside the scope of License Manager.

When assigning licenses to management processor targets, the SSH credentials for each target must be known. When deploying licenses to remote servers, the access credentials must be known. Remember that management processor licenses must be applied directly to the management processor and not its host server.

Add License page

Add License:

☒ Specify a key string: 1 - - - -

☐ Specify a file name and path: 2 3

- 1 Select the complete key string and press **Ctrl + C** to copy it.

Position the cursor in any of the five fields forming the input box and press **Ctrl + V**, or right-click your mouse to paste the license key. If the Add License function was selected after you copied the key, press **Ctrl + V** to paste the key.

The license key displays with five characters in each field.

- 2 Enter the full path and file name in the **Specify a file name and path** field.
- 3 Click **Browse**.
 - a. The **Choose file** dialog box appears.
 - b. Navigate to the file that contains the licenses to be added.
 - c. When a file has been located, click **Process**.

NOTE: When pasting in the complete key, the key can be in the normal format of five groups of five characters, with each separated by a hyphen (-), (for example, 12345-67890-54321-09876-12345). There are no spaces between the characters and the hyphens.

Key details page

Click **Process** to display the license details.

Key details:				
1 Product	2 License Version	3 License Type	4 Licenses Purchased	5 Days Max
HP Acc iSCSI Embed	1	Demo (seats and time)	10	120
			6 Back	7 Add Licenses Now

- 1 **Product**
The name of the product.
- 2 **License Version**
The license version of the product.
- 3 **Licenses Type**
The type of license for example, Demo, Beta, Duration, Site, and Maintenance.
- 4 **Licenses Purchased**
The number of licenses purchased for a product.
- 5 **Days Max**
The maximum number of days the licenses can be used.
- 6 **Back**
Returns to the **Add License** page.
- 7 **Add Licenses Now**
Adds the keys to the database.

Assigning or Applying Licenses page

Apply Licenses:

Step 2: Applying Licenses for HP Insight Dynamics - VSE suite for ProLiant

Systems can be licensed (or re-licensed) by selecting them in the following table and clicking "Apply Licenses Now".

If there are more unlicensed systems than licenses available and you have additional licenses, use the "Add Licenses" button above.

Total number of licenses available 16						Licenses Used 2		
☐	System Name	Serial Number	Unique Identifier	Status	Operating System	System Type	System IP Address	All Features Supported
☐	aaib480cs1	USM7310166	34353334-3236-5355-4037-333130313636	subscription license	Microsoft Windows Server 2003, Enterprise Edition Service Pack 2	Server	16.129.70.214	Yes
☐	aaib480cs3	USM7310165	34353334-3236-5355-4037-333130313635	subscription license	Microsoft Windows Server 2003, Enterprise Edition Service Pack 2	Server	16.129.70.205	Yes
☐	aaib480cs2	USM73702ME	34353334-3236-5355-4037-333730324045	Not licensed	Microsoft Windows Server 2003, Enterprise Edition Service Pack 2	Server	16.129.70.215	Yes

9 License advisories and warnings resulting from last licensing activity:

WARNING: Licenses indicated as required in the table below must be applied or functionality may be reduced or degraded.

System Name	Serial Number	Unique Identifier	Results
aaib480cs1	USM7310166	34353334-3236-5355-4037-333130313636	Requires license for Insight Control suite
aaib480cs3	USM7310165	34353334-3236-5355-4037-333130313635	Requires license for Insight Control suite

Apply Licenses Now

1 System Name

The name of the system where the task was executed.

2 Serial Number

A number the licensing product chooses to identify remote systems. (Check product information for specific details).

3 Unique Identifier

A unique string that further identifies a system. Systems can be licensed by any combination of system name, serial number, or unique identifier.

4 Status

The status of the use of the license on the named system.

5 Operating System

The name and edition of the operating system installed on the product.

6 System Type

The type of system licensed, for example, server, storage, or unmanaged.

7 System IP Address

The IP Address of the licensed system.

8 All Features Supported

A 'Yes' or 'No' value. Systems can be licensed with a bundle license. The Yes in this column implies that all products licensed by bundle license fully support the system indicated. No, indicates that some licenses do not support this system. You must determine which products do not support the selected system.

9 License advisories and warnings resulting from last licensing activity:

Table that indicates other licenses which are required to be in place on indicated system to fully comply with the selected product license.

License unlicensed systems (optional) page

Step 2: License unlicensed systems (optional)

Some of the selected target systems are unlicensed or licensed with a demo license. Unlicensed systems cannot be included.

If there are more unlicensed systems than licenses available and you have one or more additional licenses for this product, use the Add License or Add License from File to add these licenses, as appropriate.

System license status ①

Number of licensed systems: 0

☐	System Name	Serial Number	Status	Days Remaining	Tool Launch OK	Operating System	Model	System IP Address
☒	15.146.233.1	MY364002BH	Not licensed ②		Yes			15.146.233.1
☐	15.146.233.109	USM83808PM	Not licensed		Yes	Microsoft(R) Windows(R) Server 2003, Enterprise Edition	GhE2c Ethernet Blade Switch for HP c-Class Blade System	15.146.233.109
☐	15.146.233.191	USM83808PM	Not licensed		Yes	Microsoft Windows Server 2003, Enterprise Edition Service Pack 1	ProLiant BL460c G1	15.146.233.191
☐	15.146.233.206	USM83808PM	Not licensed		Yes	Microsoft Windows Server 2003, Enterprise Edition Service Pack 1	ProLiant BL460c G1	15.146.233.206
☐	15.146.233.33		Not licensed		Yes		HP StorageWorks MSA2012fc	15.146.233.33
☐	15.146.233.83	USM84302CU	Not licensed		Yes	Linux - VMware ESX Server	ProLiant BL460c G1	15.146.233.83

Licenses currently available ③

Total number of licenses available: 117

License Category	Licenses Available	Licenses Assigned	Licenses Used	Days Permitted	Days Remaining	License Source	Status	Updates and Upgrades	Technical Support
☐ Permanent	1	0	0			Purchased	OK	Included	Included
☐ Permanent	99	0	1			Purchased	OK	Included	Included
☐ Duration license	2	0	0	360		Purchased	No expire date as key not yet used.	Included	Included
☐ Permanent	5	0	0			Purchased	OK	Included	Included
☒ Duration license	10	0	0 ④	360		Purchased	No expire date as key not yet used.	Included	Included

< Previous Add Licenses... Add Licenses from File... Apply License ⑤ Next >

① System license status

Displays the status of system licenses, such as Not licensed, or assigned duration license.

② System selected to be licensed

System Name 15.146.233.1 is selected to have a license assigned to it.

③ Licenses currently available

Displays all of the currently available licenses to be assigned.

④ License selected

A license is selected to be assigned to system 15.148.233.1.

⑤ Apply license

Applies the selected license to the selected system.

Online license page displaying the change to both the **System license status table** and the **Licenses currently available table** after a node is licensed with **DLL** license.

Step 2: License unlicensed systems (optional)

Some of the selected target systems are unlicensed or licensed with a demo license. Unlicensed systems cannot be included.

If there are more unlicensed systems than licenses available and you have one or more additional licenses for this product, use the Add License or Add License from File to add these licenses, as appropriate.

System license status

Number of licensed systems: 1

☐	System Name	Serial Number	Status	Days Remaining	Tool Launch OK	Operating System	Model	System IP Address
☒	15.146.233.1	MY364002BH	Assigned duration license ①		Yes			15.146.233.1
☐	15.146.233.109	USM83808PM	Not licensed		Yes	Microsoft(R) Windows(R) Server 2003, Enterprise Edition	GhE2c Ethernet Blade Switch for HP c-Class Blade System	15.146.233.109
☐	15.146.233.191	USM83808PM	Not licensed		Yes	Microsoft Windows Server 2003, Enterprise Edition Service Pack 1	ProLiant BL460c G1	15.146.233.191
☐	15.146.233.206	USM83808PM	Not licensed		Yes	Microsoft Windows Server 2003, Enterprise Edition Service Pack 1	ProLiant BL460c G1	15.146.233.206
☐	15.146.233.33		Not licensed		Yes		HP StorageWorks MSA2012fc	15.146.233.33
☐	15.146.233.83	USM84302CU	Not licensed		Yes	Linux - VMware ESX Server	ProLiant BL460c G1	15.146.233.83

Licenses currently available

Total number of licenses available: 116

License Category	Licenses Available	Licenses Assigned	Licenses Used	Days Permitted	Days Remaining	License Source	Status	Updates and Upgrades	Technical Support
☒ Permanent	1	0	0			Purchased	OK	Included	Included
☐ Permanent	99	0	1			Purchased	OK	Included	Included
☐ Duration license	2	0	0	360		Purchased	No expire date as key not yet used.	Included	Included
☐ Permanent	5	0	0			Purchased	OK	Included	Included
☒ Duration license	9	1	0 ②	360		Purchased	No expire date as key not yet used.	Included	Included

< Previous Add Licenses... Add Licenses from File... Apply License Next >

① System license status

System 15.146.233.1 displays the status as having a assigned duration license.

② Licenses currently available

Displays that the Duration license has been reduced by the number of licenses assigned to system 15.146.233.1.

25 Storage integration using SMI-S

About storage systems

Storage systems are SAN-attached Fibre Channel disk arrays, switches, tape libraries, or hosts (with Fibre Channel host bus adapters). HP SIM uses [WBEM SMI-S providers](#) to discover and collect data from storage systems. To view the latest information about HP SIM device support and for information about obtaining and installing SMI-S providers, see .

The default [collection](#) **Storage Systems** is listed under **Systems by Type** in the tree in the **System and Event Collections** panel. The following collections are available under **Storage Systems**:

- **All Storage Systems** This category includes all devices that were discovered through an [SMI-S provider](#).
- **All Storage Hosts** A storage host is a server, desktop, or workstation that is connected by a HBA to a SAN. Storage hosts are also included in the **All Servers** and **All Systems** collections.
- **All Storage Switches** A storage switch is a Fibre Channel switch that is connected to a SAN. Storage switches are also included in the **All Systems** and **All Network Devices** collections.
- **All Storage Arrays** A storage array is a disk array that uses a Fibre Channel controller to connect to a SAN. Storage arrays are also included in the **All Systems** collection.
- **All Tape Libraries** A tape library is a tape drive that is connected to SAN. Tape libraries are also included in the **All Systems** collection.

NOTE: HP SIM cannot manage ESLG3, MSL, and VLS with WBEM because there is no active CVTL management on these libraries. Only SNMP is supported on these.

- **Scalable Storage Solutions**

Storage integration using SNMP

Storage devices can be broken down into real-time access and backup systems. Real-time access systems can be subdivided into internal disks, RAIDs, tape libraries, SANs, and NAS.

Most data centers have combinations of these systems including:

- **Small Business**
Almost entirely internal disk drives
- **Medium Business**
Varying combination of internal disks and RAID systems
- **Large Business**
Varying combination of internal disks, RAID, and some SAN or NAS
- **Enterprise Business**
Mostly large SAN or NAS, but some RAID and internal disks might be present

HP SIM can retrieve the information for the internal disk drives for monitored systems. This does not mean that HP SIM actively manages and configures each system previously indicated.

HP SIM can:

- Discover and identify storage systems that are directly attached to a server.
- Discover and identify storage systems that are on the network, including tape libraries.

- Receive storage system events and associate them with the system that generated the event (through Command View) running on a system, or from a tape library management card.
- Context launch appropriate management application from the context of the event or the context of the system running the Command View that generated the event.

❗ **IMPORTANT:** To discover an XP P9500 array, you can either discover it with a CVAE server or discover it with embedded SMI-S. Do not use both methods of discovery together because there are chances for Data collection and WBEM subscriptions to fail.

Storage events

With HP SIM, administrators can monitor inventory and configure and manage hardware resources and the system software that affects the systems.

HP SIM provides the administrator with a complete overview of the hardware status. Storage events provide notification that a problem exists that might affect the availability of storage resources, which can affect system and application availability. HP SIM receives detailed event messages through WBEM events or SNMP traps. These events identify the system and the affected disk and provide an error number for looking up details and a description of the problem. The event details also contain links to the Command View server that generated the event. HP SIM associates a disk or RAID subsystem with the controller managing these drives for internal storage.

Storage inventory details

HP SIM inventory retrieves and stores the following information from internal disk drives:

- Disk
 - Total number of disk slots
 - Number of used slots
 - Slot ID
 - The type of disk in slot
 - Disk manufacturer
 - Disk model
 - Disk part number
 - Disk characteristics
 - Firmware version
 - Controller ID that is managing this disk
- Controller details
 - Total number of controllers
 - Controller type
 - Controller manufacturer
 - Model number
 - Part number
 - Slot ID that this card is installed in

- Firmware version
- Controller characteristics
- RAID details
 - RAID type
 - RAID configuration
- SAN and NAS
 - Network addresses
 - Manufacturer
 - Model
- IS and MNHA
 - Part number
 - Total number of disks
 - Disk details
 - Servers being serviced by this system

Introduction to SMI-S for HP SIM

The Storage Management Initiative Specification (SMI-S) is a Storage Networking Industry Association (SNIA) standard that enables interoperable management for storage networks and storage devices. HP SIM uses this standard to discover and manage the storage systems it supports.

About SMI-S

SMI-S replaces multiple disparate managed object models, protocols, and transports with a single object-oriented model for each type of component in a storage network. The specification was created by SNIA to standardize storage management solutions. SMI-S enables management applications (such as HP SIM) to support storage devices from multiple vendors quickly and reliably because they are no longer proprietary. SMI-S detects and manages storage elements by type, not by vendor.

Key components

The key SMI-S components include:

- Common Information Model (CIM)
- Web-based Enterprise Management (WBEM)
- Service Location Protocol (SLP)

CIM

CIM, the data model for WBEM, provides a common definition of management information for systems, networks, applications, and services, and allows vendor extensions. SMI-S is the interpretation of CIM for storage. It provides a consistent definition and structure of data, using object-oriented techniques. The standard language used to define elements of CIM is Meta-Object Facility (MOF). Unified Modeling Language (UML) creates a graphical representation (using boxes and lines) of objects and relationships.

WBEM

WBEM is a set of management and Internet standard technologies developed to unify the management of enterprise computing environments. WBEM includes the following specifications:

- **xmlCIM:** Defines XML elements, conforming to DTD, which can represent CIM classes and instances
- **CIM Operations over HTTP:** Defines a mapping of CIM operations onto HTTP; used as a transport mechanism

SLP

SLP enables computers and other devices to find services in a LAN without prior configuration. SLP is designed to scale from small, unmanaged networks to large enterprise networks.

Profiles

SMI-S is organized around profiles, which describe objects relevant for a class of storage subsystem. SMI-S includes profiles for arrays, Fibre Channel HBAs, Fibre Channel switches, and tape libraries. Other storage devices (for example, NAS heads) are expected to be added in the future. Profiles are registered with the CIM server and advertised to clients using SLP. HP SIM determines which profiles it intends to manage, and then uses the CIM model to discover the actual configurations and capabilities.

SMI-S implementation

SMI-S is implemented with the following components:

- **CIM server (called a CIMOM),** that monitors WBEM requests (CIM operations over HTTP) from a CIM client, and responds to those requests.
- **CIM provider,** that communicates to a particular type of managed resource (for example, HP MSA arrays), provides the CIMOM with information about the managed resource. In theory, providers for multiple types of devices (for example, HP MSA arrays and Brocade switches) can be plugged into the same CIMOM. However, in practice, all storage vendors provide the CIMOM and a single provider together, and they do not co-exist well with solutions from other vendors.

The following components can be provided in several different ways:

- **Embedded agent**
The hardware device has an embedded SMI-S agent. No other installation of software is required to manage the device.
- **SMI solution**
The hardware or software ships with an agent installed on a host. The agent must connect to the device and obtain unique identifying information. This is the method used by all HP storage devices and most SAN devices.

About storage security using SNMP

Discovery and identification

HP SIM discovers storage systems on the LAN and Command View storage device managers running on managed systems or devices. For internal disks, the HP SIM inventory component can identify all drives installed, disk manufacturer, models, disk types, firmware revision, internal location of the drive in the system, and details about the controllers that manage the systems. For RAID drives, the RAID type (1 to 5) and manufacturer are discovered in addition to the details gathered for the internal drives. For SAN systems, HP SIM discovers the Command View servers that manage the SAN devices.

HP SIM displays storage systems as follows:

- **Internal drives**
These systems must appear in the **Properties** pages and the inventory database as components of their respective systems.
- **Tape libraries**
These devices are identified and included in the **All Systems**, **All Storage Systems**, and **All Tape Libraries** collections.
- **SAN**
The Command View systems for these devices are identified and available from the **Tools & Links** tab of the **System Page** for the systems serving the Command View systems.

NOTE: HP SIM discovers SAN and NAS management applications and provides user access to system information when those applications are started.

Prerequisites for managing storage systems

The WEBES provider must be installed on the CVEVA server to receive WBEM protocol events in HP SIM.

Procedure 30 Configuring WEBES on CVEVA proxy server

1. In WEBES, create a new protocol named CV_EVA of type **Command View EVA** under the **Managed Protocol** tab.
2. Enter the CVEVA credentials for the new protocol.
3. Set the ELMC protocol with the newly created CV_EVA protocol under **Managed Entity property**.
4. Set the **SNMP notifications (HP SIM, OVO)** under **WEBES Notification settings**.
5. Set WEBES SNMP settings by turning on **SNMP notifications** and setting the **SNMP node name** to CVEVA proxy server IP, and set **Service trap type** to type3. Apply changes.
6. Create default site in WEBES.

Using storage solutions

Event collection and launch

To receive events, the Command View software must be configured to send SNMP events to the HP SIM CMS.

For Command View SDM

Procedure 31 Configuring SNMP trap destination on Windows NT 4.0 on the Command View server

1. Select **Start**→**Settings**→**Control Panel**→**Network**→**Services**→**SNMP Service**.
The **SNMP Service Properties** dialog box appears.
2. Click **Traps**.
3. Enter a community name, such as `public`.
4. Click **Add**.
5. At the bottom of the dialog box, click **Add**.
The **SNMP Service Configuration** dialog box appears.
6. Enter the host name or IP address of the enterprise management station, and then click **Add**.
The SNMP trap destination is added.
7. Click **OK** to save the changes and close the dialog box.

Configuring the SNMP trap destination on Windows 2000

Procedure 32 Configuring the SNMP trap destination on Windows 2000

1. Select **Start**→**Settings**→**Control Panel**→**Network**→**Services**→**SNMP Service**.
The **SNMP Service Properties** dialog box appears.
2. Click **Traps**.
3. Enter a community name, such as `public`.
4. Click **Add to list**.
5. At the bottom of the dialog box, click **Add**.
The **SNMP Service Configuration** dialog box appears.
6. Enter the host name or IP address of the enterprise management station, and then click **Add**.
The SNMP trap destination is added.
7. Click **OK** to save the changes and close the dialog box.

Configuring the SNMP trap destination on HP-UX

Procedure 33 Configuring SNMP trap destination on HP-UX

1. Using a text editor, open the following file:
`/etc/snmpd.conf`
2. Insert the following information at the end of the `snmpd.conf` file:
`trap-dest: X.X.X.X`
Where `X.X.X.X` is the IP address of the enterprise management station.
3. Save and close the `snmpd.conf` file.
4. Stop the SNMP daemon by entering the following at a shell command prompt:
`ps -ef | grep snmpd`
`kill -9 PID`
Where `PID` is the process ID returned by the previous command.
5. Restart the SNMP daemon by entering the following at a shell command prompt:
`snmpd`

Loading the HSV MIB on the CMS for EVA

Procedure 34 Loading the HSV MIB on the CMS for EVA

1. On a Windows operating system, go to a command prompt.
2. Navigate to `\Program Files\HP\System Insight manager\mibs` directory.
3. Run `mxmib -a cpqhsv110v3.cfg`.

Receiving WBEM protocol events from XP arrays

CVAE must trust the HP SIM certificate. Importing and exporting the SMI-S certificates is performed by using the `HiKeytool.bat` command. This command is located at `<server install dir>\DeviceManager\Server\HiKeytool.ba`.

1. Open a shell window and execute the `HiKeytool` and select (2) for SIM-S configuration.
2. Export the management server's SMI-S certificate for indications. Refer to your management station's documentation.

3. Select (4) to import the management server's certificate into the CVAE provider's truststore for event indications. Enter the following:
 - Enter alias: Use the management server's DNS name (for example: hostname.hp.com).
 - Enter truststore-password: indtrust
 - Enter authentication-filename (absolute path): Enter path to management server's certificate file.

For additional information, refer to the *HP Storageworks P9000 and XP Event Notification* whitepaper.

Discovery

To discover an XP P9500 array, you can either discover it with a CVAE server or discover it with embedded SMI-S. Do not use both methods of discovery together because there are chances for Data collection and WBEM subscriptions to fail.

The HP SIM discovery process for systems running Command View includes the following:

- CV XP on port 80 (http)
- CV VA/SDM on port 4096 (http)
- CV TL on port 4095 (http)
- Discovery of Command View EVA is encapsulated within the discovery of the HP StorageWorks Storage Management Appliance on ports 2301 or 2381

HP SIM must be permitted to access the web server.

NOTE: To access the links to Command View, select **Tools**→**System Information**→**System Page**→**Links**.

To configure Command View and SDM:

Procedure 35 Configuring Command VIEW and SDM

1. Verify that the HP SIM CMS is within a secure IP range in the Command View server configuration.
 - **Host based**
CMS IP address included in `.../sanmgr/hostagent/config/access.dat`.
 - **Storage Area Manager management server (if applicable)**
CMS station IP address included in `/sanmgr/managementserver/config/authorizedClients.dat`.
2. Run discovery to discover or re-identify the Command View systems.
3. When discovery is complete, you can group systems in HP SIM and launch Command View from the **System Page**.

To load the EVA MIB, enter `mxmib -a cpqhsv110v3.cfg`.

NOTE: Loading the MIB could take several minutes to complete.

Configuring HP SIM with storage systems

For optimal interaction between HP SIM and [storage systems](#), complete the following procedures.

Subscribe to WBEM indication events

If a storage systems SMI-S provider supports WBEM indication events and you want to view WBEM indication events on the event table view page, you must subscribe to WBEM events for the storage system.

Viewing storage system collections

HP SIM enables you to view [storage system](#) information for collections and individual storage systems.

Procedure 36 Viewing storage system collections

1. In the **System and Event Collections** panel, expand **Systems, Shared, Systems by Type**, and **Storage Systems**.
2. Select one of the following:
 - **All Storage Systems**
 - **All Storage Hosts**
 - **All Storage Switches**
 - **All Storage Arrays**
 - **All Tape Libraries**

The system table view page for that collection appears.

Viewing individual storage systems

Procedure 37 Viewing individual storage systems

1. In the **System and Event Collections** panel, expand **Systems, Shared, Systems by Type**, and **Storage Systems**.
2. Expand the storage system collection that contains the system you want to view.
3. Click the name of the storage system you want to view.

The **System Page** for that system appears.

Viewing storage system reports

HP SIM provides predefined and customized [storage system](#) reports.

Existing storage system reports

The following predefined storage system reports are available:

- **Storage Device Capacity—All Storage Arrays**
Lists capacity usage details for all storage arrays.
- **Storage Device Controllers—All Storage Arrays**
Lists the status, port count, and number of ports utilized for each storage array controller.
- **Storage Device Inventory—All Storage Arrays**
Lists vendor, status, and port information for each storage array.
- **Storage Device Inventory—All Storage Switches**
Lists vendor, status, and port information for each storage switch.
- **Storage HBAs—All Storage Hosts**
Lists vendor, status, and port information for each host bus adapter (HBA) that is installed on a storage host.
- **Storage Logical Units—All Storage Arrays**
Lists LUN information and status for all LUNs on all storage arrays.
- **Storage Ports—All Storage Arrays**
Lists port information for all storage arrays.

- **Storage Ports—All Storage Hosts**
Lists port information for all storage host HBAs.
- **Storage Ports—All Storage Switches**
Lists port information for all storage switches.
- **Changer Devices—All Tape Libraries**
Lists the name, firmware version, and status for all tape libraries.
- **Media Access Devices—All Tape Libraries**
Lists the name, firmware version, and status for all tape libraries.

Viewing storage array capacity

HP SIM enables you to view capacity details for either a single storage array or all arrays.

Viewing storage capacity for all arrays

To view storage capacity for all arrays, run the **Storage Device Capacity-All Storage Arrays** report.

Viewing storage capacity for a single array

NOTE: Capacity information is not available for passively managed storage arrays.

Procedure 38 Viewing storage capacity for a single array

1. In the **System and Event Collections** panel, expand **Systems**, **Shared**, **Systems by Type**, **Storage Systems**, and **All Storage Arrays**.
2. Select a storage array.
3. Click the  icon next to **Capacity Information**.

26 Managing MSCS clusters

Cluster Monitor is a core component of HP SIM, and adds the ability to monitor and manage multi-node clusters. Cluster Monitor also manages multiple cluster platforms in a heterogeneous environment.

Procedure 39 Managing clusters

1. Access the **Cluster Monitor** page by using one of the following methods:
 - Method 1:
 1. Select **Tools**→**System Information**→**Cluster Monitor**.
Note: If no MSCS clusters are discovered, **Cluster Monitor** is not listed in the menu.
 2. Select a target MSCS cluster, and then click **Run Now**.
 - Method 2:
 1. Locate a cluster by expanding **Systems** under the **System and Event Collections** panel and selecting a cluster collection.
The appropriate cluster collection table appears in the workspace.
Note: Only MSCS clusters you are authorized to access appear on the cluster table view page.
 2. Choose one of the following:
 - In the **Cluster Name** column, click the name of the MSCS cluster.
 - In the **CS** column on the cluster table view page, click the MSCS cluster status icon.The **Cluster Monitor** page appears for that cluster.
2. Select from the following tabs available on the **Cluster Monitor** page. Every tab includes a **Problem Info** section that provides details about problems reported on the tab. For example, on the **Cluster** tab, this section includes status information if the cluster has a status of anything other than Normal.
Each tab also includes a **Last Update** field that displays the last time the information on the tab was updated.
 - **Cluster**
Use to view cluster information such as the cluster status, name, IP address, and quorum.
 - **Nodes**
Use to view node information such as the node status, name, and IP address.
 - **Network**
Use to view network information such as the network status, name, mask, state, role, and description.
 - **Resources**
Use to view MSCS Resource information for the cluster, including the status, name, IP address, state, group, owner node, type, and drive of the resources.

MSCS status

The **Cluster Monitor** page summarizes [cluster](#) status as defined by MSCS and lists the status and values of MSCS-defined cluster attributes.

Cluster fields

Table 13 Cluster fields

Name	Description
Status	Status of the cluster: Normal (the cluster condition is functioning normally, every node condition and resource condition is normal), Degraded (the cluster condition is degraded if at least one node condition is failed or degraded or at least one resource condition is degraded), Failed (the cluster condition is failed if every node condition is failed or at least one resource condition is failed), and Other (the cluster condition cannot be determined and every node condition and resource condition is undetermined)
Name	Name or alias for the cluster
IP	IP address of the cluster alias
Quorum	Resource that maintains essential cluster data and guarantees that all nodes have access to the most recent database changes

Node fields

Table 14 Node fields

Name	Description
Name	Name or alias for the node
Status	Status of the node: Normal (the node status is an active cluster member), Degraded (the node status is down, trying to form or rejoin a cluster, is operating as an active member of a cluster but cannot host any resources or resource groups, or is up but cluster activity is paused), Failed (the node status is down or trying to form or rejoin a cluster), and Other (the node status is unavailable or could not be determined)
IP	IP addresses associated with the node

NOTE: No information appears in the IP field of a particular node if an Insight Management Agent 4.22 or earlier is installed on that node in the cluster.

Cluster Monitor shows the condition of Other when all the nodes of a cluster are down.

Network fields

Table 15 Network fields

Name	Description
Name	Server cluster object that carries internal communication between nodes and provides client access to cluster resources
Status	Status of the network: Normal (the network state is online or available), Degraded (the network is partitioned), Failed (the network state is offline), and Other (the network state indicates that an error has occurred and the exact state of the network could not be determined or the network state is unavailable)
Mask	The subnet mask associated with the network within the cluster
State	State of a particular network in the cluster: Offline (not operational), Partitioned (operational, but two or more nodes on the network cannot communicate), Online (operational), or Unavailable (information is not available)
Role	Role the network name plays in the cluster: network name for the cluster, network name for computer systems in the cluster, or network name for groups in the cluster
Description	Description of the network

Resource fields

Table 16 Resource fields

Name	Description
Name	Physical or logical entity that is capable of being owned by a node, brought online and taken offline, moved between nodes, and managed as a server cluster object
Status	Status of the resource: Normal (the resource state is online), Degraded (the resource state is Unavailable, Offline, Online Pending, or Offline Pending), Failed (the resource state is failed), and Other (unable to determine the resource condition)
Group	Collection of resources managed as a single server cluster object
OwnerNode	Node on which a resource resides
Type	Server cluster object used to categorize and manage resources that have similar characteristics
Drive	Disk or drive on which the resource resides

NOTE: A group must have a network name and an IP address associated with it for you to access group resources. A group can be owned by any node in the cluster and can be moved by users with [administrative rights](#) for load balancing and other administrative purposes. When a failure takes place, the entire group fails over, which prompts the cluster software to transfer all group resources and data to a different node in the cluster. The resources and data in a transferred (failed over) group are still accessible under the same network name and IP address, even after they have been moved to a different node.

Cluster Monitor resource thresholds

[Cluster resources](#) use [thresholds](#) to trigger HP SIM events. The Disk resource sets thresholds for disk capacity, and the CPU resource sets thresholds for CPU utilization.

Disk capacity thresholds

Use the Disk resource to collect disk capacity data. To access the **Cluster Monitor - Node Resource Settings** page where the thresholds are set, select **Options**→**Cluster Monitor**→**Node Resource Settings**.

The threshold values you enter in the **Settings for the Selected Resource** section define the Minor, and Major ranges for disk utilization on monitored nodes.

For each disk, there are four thresholds in pairs. The Minor and Major thresholds are associated with a corresponding reset threshold. Utilization enters the Major range when it equals or exceeds the Major threshold value. It remains in the Major range until it falls to or below the Major reset value. Minor and Major reset thresholds behave similarly.

You can specify different thresholds for each disk in each node of a cluster.

CPU utilization thresholds

Use the CPU resource to collect utilization data for CPUs in a cluster. To access the **Cluster Monitor - Node Resource Settings** page where the thresholds are set, select **Options**→**Cluster Monitor**→**Node Resource Settings**.

The threshold values you enter in the **Settings for the Selected Resource** section define the Normal, Minor, and Major ranges for CPU utilization on the selected node.

For each CPU, there are four thresholds in pairs. The Minor and Major thresholds are associated with a corresponding reset threshold. Utilization enters the Major range when it equals or exceeds

the Major threshold value. It remains in the Major range until it falls to or below the Major reset value. The Minor and Major reset thresholds behave similarly.

You can specify different thresholds for each CPU in each node of a cluster.

Cluster resources supported by HP SIM

HP SIM supports the following Cluster Monitor resources:

- **Disk and CPU resources**

Monitor disk capacity and CPU utilization, respectively. You can set minor and major thresholds for nodes in a cluster. When those thresholds are reached, Cluster Monitor creates an HP SIM event. The event triggers associated e-mail and paging notification as configured in HP SIM options.

- **System**

Monitors the system health of the cluster member.

Cluster Monitor states

NOTE: The cluster condition is Other when all nodes of a cluster are down.

List	Normal	Degraded	Failed	Other
Node	The node status is an active cluster member.	The node status is down, is trying to reform or rejoin a cluster, is operating as an active member of a cluster but cannot host resources or resource groups, or is up but cluster activity is paused.	The node status is down or is trying to form or rejoin a cluster.	The node status is Unavailable or could not be determined.
Network	The network state is Online or Available.	The network state is Partitioned.	The network state is Offline.	The network state indicates that an error occurred and the state of the network could not be determined, or the network state is unavailable.
Resources	The resource state is Online.	The resource state is Unavailable, Offline, Online Pending, or Offline Pending.	The resource state is Failed.	The resource state is Unknown.

NOTE: For additional information about the MSCS, see Microsoft documentation.

Cluster Monitor polling rate

NOTE: You can specify only one polling rate (interval) for all nodes in all [clusters](#). You cannot specify different rates for different nodes, so the polling fields appear on the configuration page only when you select **All** in both **Cluster** and **Node** dropdown lists.

CPU polling rate

The CPU polling rate determines how often Cluster Monitor checks CPU utilization as reported by the appropriate Insight Management Agent on monitored nodes.

Adjust the CPU polling rate by configuring the Cluster Monitor node resource settings.

Disk polling rate

The Disk polling rate determines how often Cluster Monitor checks the free disk space as reported by the appropriate Insight Management Agent on monitored nodes.

Adjust the polling rate by configuring the Cluster Monitor node resource settings.

MSCS status polling rate

The polling rate you enter determines how often Cluster Monitor checks the MSCS status of monitored clusters.

Adjust the status polling rate by configuring the Cluster Monitor's cluster resource settings.

System status polling rate

The system polling rate determines how often Cluster Monitor checks node status as reported by the appropriate Insight Management Agent running on the nodes.

System is a node-level attribute. You can adjust the polling rate by configuring Cluster Monitor node resource settings. The polling rate is a global attribute of the resource, so you can specify only one polling interval for all nodes in all clusters. The polling fields appear on the configuration page only when you select **All** in both the **Cluster** and **Node** dropdown lists.

27 HP SIM Audit log

HP SIM logs all [tasks](#) performed by all HP SIM users on all systems. The information is stored in the Audit Log file on the CMS. Several features of the HP SIM Audit Log are configurable. For example, you can specify which tools log data and the maximum Audit Log file size. The HP SIM Audit Log is configured through the `log.properties` file, and tool logging is enabled or disabled through the XML tool definition files.

On Windows, the audit log can be found at the `<SIM installdir>/logs/mx.log`. On Linux and HP-UX, the audit log can be found at `/var/opt/mx/logs/mx.log`. These are rolled over to `mx.log.old` when the file reaches the maximum default size of 20 MB.

Configuring the HP SIM audit log

Configuring the HP SIM Audit log is performed from the CLI, and you must be signed-in as root or administrator.

Configuring the tool definition files

The XML tool definition file provides an option to disable logging of SSA and MSA command tools. The log attribute for the command element specifies whether the results of the command are output to the HP SIM log file. Command output is logged by default.

Configuring the log.properties file

You might need to create the file and name it `log.properties` if one does not exist in the directory. HP SIM uses default values when the file does not exist or when a variable is not defined in the file.

For Windows, the file is located in `<SIM installdir>/logs/mx.log`.

For Linux and HP-UX, the file is located in `/var/opt/mx/logs/mx.log`. This is rolled over to the `mx.log.old` file when it reaches the maximum configured size of 20MB.

The file is rolled over to the `mx.log.old` file when it reaches the maximum configured size of 20MB.

Viewing the audit log

HP SIM logs all tasks performed by all HP SIM users on all systems. The information is stored in the Audit Log file on the CMS.

NOTE: You must be signed-in as root or administrator (or any user with administrative rights) to read the audit log file directly.

Procedure 40 Viewing the HP SIM audit log

1. Select **Tasks & Logs**→**View Systems Insight Manager Audit Log**. The **Audit Log** page appears.
2. Select the log entries you want to view by selecting one of the following options:
 - **most recent 40 entries**. Select this to view a selectable number of the most recent log entries. The default is set to view the 40 most recent log entries.
 - **from entry " " to entry " "**. Select this option to view an indexed range of log entries.
3. Click **View Now**. The requested log entries appear.

Example audit log

```
Example Audit Log: User "partner" runs tool "ls" on cup11.hp.com from cup12.hp.com
from CMS cup12.hp.com
```

```

104611: 2008-04-24 11:17:45
PDT,JOB,PROGRESS,START,JOB,44641_cup12.hp.com,VERBOSE,partner,,,
Running Tool:ls
Expanded Command Line:ls
Targets:
cup11.hp.com

104612: 2008-04-24 11:17:45
PDT,JOB,PROGRESS,START,JOB,44641_cup12.hp.com:cup11.hp.com,
DETAIL,partner,,,
Running Tool:ls

104613: 2008-04-24 11:17:45
PDT,JOB,SUCCESS,DONE,JOB,44641_cup12.hp.com:cup11.hp.com,
DETAIL,partner,,,
Running Tool:ls
Exit Code:0

```

Log content

The HP SIM Audit Log contains the following information in the order listed, and the log entry key @!@ precedes all other fields in an audit log entry.

- Time stamp date, time, and time zone
- Category
- Result
- Action
- Object type
- Object type descriptor
- Level
- Session user login string
- (Optional) Session ID
- (Optional) Transaction ID
- (Optional) Session user full user name

These fields appear in one line. If messages or additional information about a log entry is present, it appears in the next line.

28 HP Version Control and HP SIM

About the Version Control Agent

The HP VCA is an Insight Management Agents installed on a system that enables you to view HP software and firmware installed on the system. You can configure: HP VCA to point to a [repository](#) managed by HP VCRM, enabling easy version comparison and [software updates](#) from the repository to the system where HP VCA is installed.

HP VCA provides [version control](#) and system update capabilities for a single HP system. HP VCA determines system software status by comparing each [component](#) installed on the local system with the set of individual components or a specified ProLiant and Integrity Support Packs listed in HP VCRM. While browsing to HP VCA, you can update individual components or an entire ProLiant and Integrity Support Packs by clicking the install icon located next to the system software status icon.

HP VCRM and HP VCA are integrated with HP SMH, which is the standard single-server management tool in the HP Foundation Pack. HP SIM, also part of the HP Foundation Pack, uses HP VCRM and HP VCA to facilitate software versioning, update, and tasks related to it.

HP VCA is available for Windows and Linux operating systems. HP VCA is an integrated part of HP SMH and displays the [available software](#) inventory of the system it is installed on. HP VCA also allows the installation, comparison, and update of system software from a repository managed by HP VCRM.

Users with administrator or operator privileges can access the HP VCA to maintain the [software inventory](#) of the system. The installation of components and configuration activities are logged to a log file on the system. [HP VCA logs](#) activities, such as software installations. However, installations done outside HP VCA do not appear in this log.

HP VCA enables you to view software installed on selected HP equipment, available updates, and whether the installed software complies with the latest updates in the selected repository. In addition, you can add or update HP software on the system remotely, using the browser interface of HP VCA.

You can use the [Replicate Agent Settings](#) feature in HP SIM to update multiple servers with HP VCA settings.

HP VCA enables the following tasks:

- Viewing installed software
- Selecting an HP VCRM as a reference point for obtaining software updates
- Selecting a ProLiant and Integrity Support Packs as a managed baseline
- Viewing details of a ProLiant and Integrity Support Packs or software component that is in the HP Version Control repository
- Installing a ProLiant and Integrity Support Packs or software component from the HP Version Control repository
- Printing the installed software inventory and software status
- Managing the HP VCA log

In addition to maintaining the software inventory of the system, the HP VCA integrates with HP SIM, enabling administrators to take advantage of the Software Update capabilities of the agent.

Additional resources

For additional resources, go to <http://www.hp.com/servers/manage>.

About the Version Control Repository Manager

HP VCRM is an HP Insight Management Agents that manages a directory of HP software and firmware components. You can use HP VCRM without [HP VCA](#) to provide a listing of available software and firmware to load on the local machine. HP VCRM is part of the HP Foundation Pack. HP VCRM is designed to be used in a one-to-many configuration with a HP VCA installed on each managed HP system to manage installed HP software and firmware. In conjunction with HP SIM, HP VCRM, and HP VCA provides enterprise management of HP software and firmware on HP ProLiant and Integrity systems. Alone, HP VCRM can catalog and manage a repository of ProLiant and Integrity Support Packs and software and firmware for HP ProLiant and Integrity systems.

NOTE: Although you can install ProLiant and Integrity Support Packs or [component](#) to the local machine using HP VCRM, you cannot install the software on remote servers unless HP VCA is installed on the remote server and using HP VCA.

HP VCRM permits the following tasks:

- Viewing the contents of the repository
- Configuring Automatic Update to deliver ProLiant software from HP as it becomes available
- Uploading a support pack to the repository from a CD or other accessible media using the **Upload a Support Pack** feature
- Creating ProLiant and Integrity Support Packs
- Deleting ProLiant and Integrity Support Packs and components
- Copying ProLiant and Integrity Support Packs and components to another repository
- Configuring components in the repository that are flagged as requiring configuration
- Updating from HP.com now
- Rescanning the repository and rebuilding the catalog
- Managing the log
- Installing selected components at the local (browser client) system

About integration

For software versioning and updating, HP SIM relies on HP VCRM and HP VCA. By using these applications, HP SIM provides a single view of the software status for managed ProLiant or Integrity servers, and it can update software and firmware on those servers through its powerful query and task features. Updates can be scheduled and applied to specific sets of servers based on predetermined criteria, including applying updates only to systems that require an update.

NOTE: HP SIM no longer requires the VCA to be installed on target systems. The new SW/FW Baselines feature performs this task.

To take full advantage of the software update capabilities of HP SIM, verify that the following conditions are met:

- Every managed target server on the network has the HP VCA installed and is configured to use a repository.
- Every repository that is to be used has the HP VCRM installed.
- You can optionally use the automatic update feature of the HP VCRM to automatically update all repositories with the latest software from HP.

About software repositories

Updating ProLiant Support Packs and components using HP VCRM from a single or multiple repositories saves time and is key to standardizing software maintenance and update procedures on distributed [systems](#).

For maximum manageability and flexibility across operating system platforms, each repository you create must conform to the following conditions:

- It must be located on a local drive with write access.
- It must be updated automatically by the HP VCRM.
- It must be managed by HP VCRM.

After a repository is created, it must be populated with ProLiant Support Packs and components before being updated on target HP systems. Although it is optional, the easiest and most efficient way to update a repository is by using the Automatic Update feature of HP VCRM. This feature enables you to schedule an automatic population of the repository. However, the repository can be updated in one or more of the following ways:

- By using the Automatic Update feature of HP VCRM
- By using the Upload ProLiant Support Pack feature of HP VCRM, which enables users to easily copy ProLiant Support Packs from a SmartStart CD or other accessible media
- By manually downloading the software into the repository from <http://www.hp.com/go/softwaredepot>

About multiple system management

The Software Update capabilities of HP SIM includes the following features:

- **Install Software and Firmware.** Use to automatically update ProLiant Support Packs and components on HP systems managed by HP SIM. The target systems must have HP VCA installed.
- **Searching by systems with Software/Firmware.** Use to create and display a list of systems with specific software or firmware versions. For example, a user with [administrative rights](#) might want to locate and display HP systems with Insight Management Agent earlier than a defined version. The search can then be used with the Install Software and Firmware Task to update the systems to the current version of Insight Management Agent.

The Install Software and Firmware task can be executed in two modes:

- **Offline mode**
Offline task is executed on a baremetal sever (server with no operating system installed) and only supported firmware components are installed on the server. The target system for this task is the iLO of the server.
- **Online mode**
This task installs all supported software and firmware components on the server.
- **Software Version Status Polling.** Use to retrieve software and firmware upgrade statuses from HP VCA on target systems. Software and firmware inventories are also retrieved from those systems during this task.
- **Replicate Agent Settings.** Use to have HP SIM to retrieve Web Agent configuration settings from a source device and distribute that configuration to target systems through their Web Agents.

These capabilities rely on the integration of HP SIM with HP VCRM and HP VCA.

NOTE: When software/firmware for a component is not available in the baseline, then it will be shown blank. If junk or blank values are found to be listed in the **Software Firmware Baselines** section, it is because the description for the component is not found by the providers. You can verify this by going through the Data Collection reports.

The junk values are unique identifiers for the component which do not have descriptions. The junk values are numbers in sequential order prefixed with a hyphen (-).

Often, multiple components have the same descriptions. Therefore, the component name is prefixed with a hyphen, followed by the number in sequential order, followed by the component description.

29 Compiling and customizing MIBs

HP SIM; provides the capability of managing systems through SNMP and by receiving incoming SNMP trap events. HP SIM ships with many MIBs pre-configured. For a complete list, see [“Out-of-the-box MIB support in HP SIM” \(page 229\)](#). You can use tools provided by HP SIM to integrate third-party (non-HP) SNMP v1/v2/v3 MIBs into HP SIM and to provide support for processing and displaying traps from other systems. The MIB syntax extensions supported by HP SIM provide additional value in customizing specific trap information. Finally, the set of MIBs included with HP SIM to provide out-of-the-box support for many HP systems.

Integration of third-party MIBs is a topic for advanced users of HP SIM. Most vendors tend to loosely follow industry standards for the development of MIBs and MIB compilers. Therefore, it is often the case that MIBs require some changes and customization on the part of the end-user to properly integrate the MIBs with a management application such as HP SIM.

This chapter frequently references directories and tool locations throughout the HP SIM directory structure. This directory structure varies depending upon your installation choices and on the operating system under which you have installed HP SIM. Typical installation paths are as follows:

Windows

- C:\Program Files\HP\System Insight Manager\ as the <BASE> installation directory
- C:\Program Files\HP\System Insight Manager\mibs for all MIB and CFG files
- C:\Program Files\HP\System Insight Manager\lbin for mcompile
- C:\Program Files\HP\System Insight Manager\bin for mxmib

HP-UX and Linux

- /opt/mx as the <BASE> installation directory
- /opt/mx/mibs for all MIB and CFG files
- /opt/mx/bin for mcompile and mxmib

NOTE: Compiling MIBs into HP SIM only enables the console to receive SNMP traps from systems. This does NOT extend the data collection mechanism to collect data points from the compiled MIBs into the database. This type of functionality is currently not available in HP SIM.

MIB management tools

HP SIM provides three tools for use with MIB integration and trap customization. MIBs are registered with HP SIM using two command-line tools. These tools are only accessible to the administrator or root user of the operating system. They are:

- mcompile
- mxmib

In addition, HP SIM provides a GUI tool to display and edit the trap settings for MIBs already compiled using the command-line tools listed above. This tool is the **SNMP Trap Settings** page. The remainder of this section discusses each of the tools provided and elaborates on their specific usage.

mcompile

The `mcompile` tool verifies the syntax of all MIBs to be loaded into the system. `mcompile` resolves all MIB dependencies and, where necessary, converts SNMP v2/v3 MIBs into v1 format for loading into the HP SIM database. `mcompile` is located in the <BASE>\lbin directory and should be run from the <BASE>\mibs directory. `mcompile` looks for all MIB files in the <BASE>\mibs

directory by default so any MIB that you intend to register should be copied to the <BASE>\mibs directory. While `mcompile` does provide some capability to specify a different directory to search for MIBs, as a best practice HP strongly recommends you place all MIBs in the <BASE>\mibs directory. Usage for `mcompile` is as follows:

```
mcompile [-d <dirsSpec>] <mibfile></
```

Use of the `-d` switch is not necessary when you have copied all MIBs, including dependency MIBs, to the <BASE>\mibs directory and execute `mcompile` from the <BASE>\mibs directory. The `-d` switch specifies which directory contains the MIB files to be compiled into HP SIM. The directory path must be specified as relative to the full path or relative to the <BASE> directory.

As output, `mcompile` produces a CFG file and save it to the <BASE>\mibs directory. This file has the same name as the source MIB except it has the `.cfg` suffix. In the typical usage mentioned above, the resulting output file would be `test.cfg`. Running `mcompile` several times against the same source MIB produces multiple revisions of the CFG with the latest version retaining the `.cfg` extension. CFG files are stripped-down versions of the original source MIBs where all comments have been removed, all imports from other MIBs have been resolved and substituted as needed, and the compiler has converted v2/v3 syntax to v1 where appropriate.

When compiling MIBs with dependencies, the dependent MIB must be located in the same directory as the target MIB and must follow a certain naming convention, typically `MIBMODULE.MIB`. An example follows using excerpts from the CPQFCA MIB:

```
CPQFCA-MIB DEFINITIONS ::= BEGIN
IMPORTS
    compaq
FROM CPQHOST-MIB
    enterprises
FROM RFC1155-SMI
    DisplayString
FROM RFC1213-MIB
    OBJECT-TYPE
FROM RFC-1212
    TRAP-TYPE
FROM RFC-1215
    cpqSsChassisName
FROM CPQSTSYS-MIB
```

`mcompile` searched for `compaq` by opening the file `CPQHOST.MIB` and `mcompile` looks for `cpqSsChassisName` in `CPQSTSYS.MIB`. The other imports are resolved automatically when `mcompile` runs from the <BASE>\mibs directory. HP provides versions of the RFC 1212, 1213, and 1215 MIBs for automatic import during compilation. `mcompile` automatically resolves and imports internally from RFC1155.

Another example of imports during compilation comes from the `BLADETYPE2-TRAP.MIB` used by the HP ProLiant BL p-Class GbE2 Interconnect Switch:

```
BLADETYPE2-TRAP-MIB DEFINITIONS ::= BEGIN
IMPORTS
    TRAP-TYPE
FROM RFC-1215
    sysName
FROM RFC1213-MIB
    hpSwitchBladeType2-Mgmt
FROM HP-SWITCH-PL-MIB
    agSlotNumber
FROM BLADETYPE2-SWITCH-MIB
    ipCurCfgGwIndex
FROM BLADETYPE2-NETWORK-MIB
```

In this example, *TRAP-TYPE* and *sysName* are readily resolved as in the example above. *hpSwitchBladeType2-Mgmt* is resolved by *mcompile* checking *HP-SWITCH-PL.MIB*. *agSlotNumber* is resolved from *BLADETYPE2-SWITCH.MIB* and *ipCurCfgGwIndex* is resolved from *BLADETYPE2-NETWORK.MIB*.

To illustrate further how imports are resolved — the following procedure is how *mcompile* would attempt to resolve the import for *hpSwitchBladeType2-Mgmt*:

Procedure 41 How MIB imports are resolved

1. Search for a file named *HP-SWITCH-PL-MIB.mib* (module name, uppercase).
2. Search for a file named *HP-SWITCH-PL.mib* (module name without *-MIB*, uppercase).
3. Search for *hp-switch-pl.mib* (convert name to lowercase for case sensitivity in Linux/HP-UX).
4. Search for *hp-switch-pl.mib.mib* (convert name to lowercase for case sensitivity in Linux/HP-UX).
5. Report an error indicating that the imported MIB could not be found.

A major consideration when importing MIBs is locating variables from other third-party MIBs. In many cases, MIBs are named to match module names. However, in some circumstances it might be necessary to rename MIB files to match the module names prior to compilation. For example, some vendors might provide MIB files with different extensions such as *.my*. In this case, before using *mcompile*, the *mibfile.my* file must be renamed to *mibfile.mib*.

mxmib

The *mxmib* tool registers MIBs into the HP SIM database by using their corresponding CFG files. This tool has the capability to list all registered MIBs, to display a list of traps contained in each individually registered MIB, and to unregister MIBs that you or the system have previously registered.

- ❗ **IMPORTANT:** While it is possible to unregister MIBs currently registered in the HP SIM database, HP strongly advises you do not unregister any files that have been registered by default. Doing so can impair HP SIM's ability to correctly process traps from other HP systems on the network.

If you unregister a MIB from HP SIM, the corresponding received events in HP SIM are automatically deleted.

mxmib expects to find all files located in the *<BASE>\mibs* directory. Usage for *mxmib* is as follows:

```
mxmib -a <myfile.cfg>
mxmib -f <mylist.list>
mxmib -l
mxmib -t <myfile.mib>
mxmib -d <myfile.mib>
```

The switches work as follows:

- *-a* registers a new CFG, *<myfile.cfg>*, or replaces the data of a previously registered MIB.
- *-f* reads and processes a list of CFGs from a file, *<mylist.list* (one *mibName* per line)>, to register with HP SIM. This file must reside in the *<BASE>\mibs* directory and the full CFG filename must be listed on individual lines. Each line in the file is processed as it would be by running the *mxmib -a* command individually on each individual MIB file.
- *-l* lists all the MIBs registered in HP SIM. Supplying no arguments to *mxmib* defaults to running *mxmib -l*.
- *-t* lists the traps in the specified MIB *<myfile.cfg>*.
- *-d* unregisters a MIB, *<myfile.cfg>*, from the HP SIM database.

The initial command to register the file uses the `.cfg` extension, but all subsequent commands refer to the file by its `.mib` extension.

- ❗ **IMPORTANT:** `mxmib` is order sensitive. While the command enables you to compile MIBs whose dependencies have not been compiled, for optimal results, HP recommends that you register MIBs with HP SIM in order of dependency. If you do not compile MIBs in order of dependency, HP SIM might not properly resolve varbind data for incoming traps from MIB X when a varbind has been imported from MIB Y that was not registered prior to registering MIB X. MIB dependencies are typically identified at the top of MIB files in the `IMPORTS` section and are discussed in the `mcompile` section. Note that failing to compile imported MIBs properly does not block reception of traps; it only limits the data captured for some traps.

mxmib MIB keyword customization

After using `mcompile` to parse and validate the source MIB, you can customize the resulting CFG file for support in HP SIM. Specifically, there are special keywords that can be defined on a per-trap basis. At the conclusion of this section, there is a full example. The keywords and their usage are as follows.

--#TYPE

The `TYPE` keyword provides a way to add a short description of the trap to HP SIM. This short description can be used when sending a paging message. This enhances the ability to transmit information without being verbose. This keyword does not provide any functional purpose; however, it does represent the primary display string for the trap when it is displayed in HP SIM. Note that while the `TYPE` field does not need to be unique, but HP recommends that the combination of `TYPE` and `CATEGORY` fields form a unique pair so that this event can be effectively searched for using the Event by Category/Type search criteria.

--#SEVERITY

The `SEVERITY` keyword can be used to alter the severity of a trap. The vendor who created the MIB might have decided that the trap, under most circumstances, only warrants a severity level of informational. However, you might need to escalate the trap's severity based on operational importance. Therefore, this keyword overrides default severity. The allowable severity levels are shown below. Many vendors have different severities specified in their MIBs such as Normal, Warning, Degraded, Broken, and so on. These severities must be changed in the base MIB or CFG to one that matches HP SIM. For example, Degraded can be mapped to Minor or Major, depending on the degradation. Editing the MIB or CFG and doing a search/replace on the severities is the easiest way to tweak the MIB. HP SIM also provides a GUI to change the `SEVERITY` after MIB compilation.

- **INFORMATIONAL**

Events of this type require no attention. They are provided as useful information.

- **MINOR**

Events of this type indicate a warning condition that can escalate into a more serious problem.

- **MAJOR**

Events of this type indicate an impending failure.

- **CRITICAL**

Events of this type indicate a failure and signal the need for immediate attention.

--#ENABLE

The `ENABLE` flag can be set to `TRUE` or `FALSE` and can effectively enable or disable a trap from being processed by HP SIM. The usage for the keyword is either `TRUE` to indicate that the trap should be processed or `FALSE` to indicate that this trap should not be processed. By default, this keyword is `TRUE` and should only be explicitly overwritten on an exception basis.

--#CATEGORY

This provides a categorization of the trap for ease of viewing and use in forming HP SIM lists. You can use predefined categories or, if none of these fit your need, you can create a category befitting your circumstances. The HP SIM **SNMP Trap Settings** page provides a GUI to change the *CATEGORY* after MIB compilation. The predefined categories in HP SIM are shown below.

- APPLICATION
- ARCserve Events
- CommandView Events
- Common Cluster Events
- Cpqdsccs
- Data Protector Events
- General Backup
- Giga Switch Events
- HP Open View Internet Services Events
- HP OVSAM Events
- HP Service Events
- HP-UX EMS Events
- Integrity Server Events
- IO Drive Events
- NetServer Events
- PATROL Events
- PowerDevice
- ProLiant Application Events
- ProLiant BL p-Class GbE Interconnect Switch Events
- ProLiant BL p-Class GbE2 Interconnect Switch Events
- ProLiant Cluster Events
- ProLiant Miscellaneous Events
- ProLiant NIC Events
- ProLiant Operating System Events
- ProLiant Rack Events
- ProLiant Remote Management Events
- ProLiant Storage Events
- ProLiant System and Environmental Events
- ProLiant UPS Events
- RFC 1215 SNMP Trap Events
- SAN Appliance Events
- Server Net Events
- ServiceGuard Events
- STORAGE
- SWCC Events

- SYSTEM AND ENVIRONMENTAL
- Tandem EMS Events
- TruCluster Events
- Unassigned
- Unisys Configuration Agent Events
- UNKNOWN
- WYSE Events
- ZESA
- ZHRM

--#MSG_FORMATTER

This keyword has a number of HP SIM specific commands. These commands are parsed and executed when a paging or e-mail Automatic Action on Event rule is created and exercised within HP SIM. You might view these commands as a paging or e-mail command language. The general layout of each command contains an operand and descriptive text associated with the operand. The descriptive text must be delimited by a # pair. If the parser within HP SIM does not recognize a command, it will disregard that command without providing any additional feedback.

- ❗ **IMPORTANT:** Changing the `MSG_FORMATTER` string is only recommended for extremely advanced users. Always back up any files that are modified so that they can easily be restored. Also, for HP ProLiant traps, HP has already generated intelligent messages that are registered by default with HP SIM.

Referring to the following tables, the `V` keyword represents varbind information specific to individual traps. Numerically, all `V` definitions match the varbinds as they appear in the trap.

Table 17 Varbind keywords and descriptions

Keyword	Description	Comments
<code>\$VnV#Some text#</code>	Includes value for varbind and descriptive text (in this case, <i>Some text#</i>)	Label will reflect the value selected. This will vary on a trap-to-trap basis.
<code>\$VnD#Some text#</code>	Includes the varbind description that is only available within HP SIM	Label will reflect the value selected. This will vary on a trap-to-trap basis.
<code>\$Hdr#Some text#</code>	Used to add text or formatting to headers	Text that could be added to add clarity to output data. Used to form varbind data into text sentences.

Also, if the beginning keyword in the trap definition file is a `$!`, that tells the HP SIM parser to disregard the global settings and to use only the trap definition file keywords. See example below.

```
cpqDa5PhyDrvStatusChange TRAP-TYPE
ENTERPRISE compaq
VARIABLES { sysName, cpqHoTrapFlags, cpqDaPhyDrvStatus,
cpqDaPhyDrvCntlrIndex, cpqDaPhyDrvBusNumber,
cpqDaPhyDrvBay, cpqDaPhyDrvModel, cpqDaPhyDrvFWRev,
cpqDaPhyDrvSerialNum, cpqDaPhyDrvFailureCode }
DESCRIPTION "Physical Drive Status Change. This trap signifies
that the agent has detected a change in the status of an
HP Drive Array physical drive. The variable cpaDaPhyDrvStatus
indicates the current physical drive status. User Action: If the physical
drive status is failed(3) or predictiveFailure(4), replace the drive."

--#TYPE "Physical Drive Status Change"
--#SUMMARY "Physical Drive Status is now %d."
--#ARGUMENTS {2}
```

```
--#SEVERITY CRITICAL
--#TIMEINDEX 99
--#MSG_FORMATTER "$V1V#Computer: # $V3V#Drive Status: # $V9V#Serial Number: #"
:= 3029
```

The e-mail or pager output would appear as:

```
Event Notice ID: 3029
Computer: CRONUS
Drive Status: FAILED
Serial Number: WS7000134715
Event Description: Physical Drive Status Change.
This trap signifies that the agent has detected a change in
the status of an HP Drive Array physical drive. The variable
cpaDaPhyDrvStatus indicates the current physical drive status.
User Action: If the physical drive status is failed(3) or
predictiveFailure(4), replace the drive.
Event Time: 01/09/2003 15:46: PM
```

Event Notice ID, Event Description and Event Time are inserted by HP SIM into all event notifications and that Computer (V1, sysName), Drive Status (V3, cpqDaPhyDrvStatus) and Serial Number (V9, cpaDaPhySerialNum) are customized to this specific trap.

Using the preceding example and adding the \$!

```
--#MSG_FORMATTER "$! $V1V#System Name: # $V3V#Drive Status: # $V9V#Serial
Number: #"
```

The e-mail or pager output would be:

```
System Name: CRONUS
Drive Status: FAILED
Serial Number: WS7000134715
```

Using the \$Hdr keyword in conjunction with \$! to further customize the display could be as follows:

```
--#MSG_FORMATTER "$! $Hdr#The # $V1V#system # $Hdr#had the following #
$V3V#Drive Status:# $Hdr#. The system Serial Number # $V9V#is #
$Hdr#.#"
```

The e-mail or pager output would be:

The system Cronus had the following Drive Status: failed. The system Serial Number is WS7000134715

-
- ① **IMPORTANT:** For the TYPE, CATEGORY, and MSG_FORMATTER keywords described above, the value for these keywords must be encapsulated in quotes, such as xxx for the mxmib to successfully register the MIB in question. Other keywords such as SEVERITY and ENABLE do not require quoted values.
-

SNMP Trap Settings page

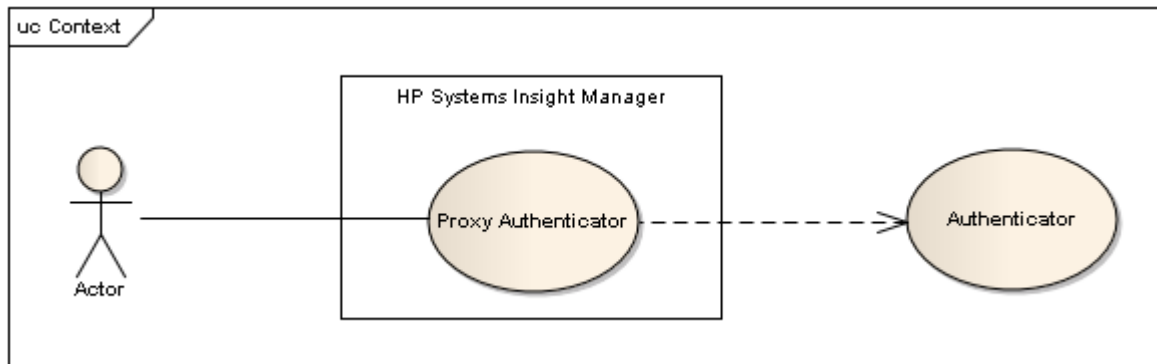
The **SNMP Trap Settings** page has the capability to modify the attributes of any trap that has been registered with the HP SIM database. The attributes that are available for modification include the short and long descriptions, severity, category, and the trap enable/disable flag. Use the interface on this page to first select the registered MIB containing the trap in which you are interested, and then select the specific trap you wish to modify.

Fields can be modified as follows:

- The **Description** field is the long description stating the nature of the trap. The **Description** field is used on the **Event detail** page and can be included in paging and e-mail notifications. This field corresponds to the *DESCRIPTION* keyword in the CFG files.
- The **Event Type** field is the short description and is used as the display string when viewing a list of events. The event type can also be used as part of a paging or e-mail notification. Event type fields have been custom-created for all of the HP ProLiant hardware events. However, for many other MIBs they have not been customized. Tailoring this field to present a clear message is crucial for presenting meaningful event data in HP SIM. This field corresponds to the *#TYPE* keyword in the CFG files.
- The **Severity** field can be set to CRITICAL, MAJOR, MINOR, or INFORMATIONAL. The default is INFORMATIONAL when no other severity has been set by the base MIB. Many vendors have different severities specified in their MIBs such as Normal, Warning, Degraded, Broken, etc. These severities need to be changed in the base MIB or CFG to one that matches HP SIM. For example, Degraded can be mapped to Minor or Major, depending on the degradation. Editing the MIB or CFG and doing a search/replace on the severities is the easiest way to tweak the MIB. This field corresponds to the *#SEVERITY* keyword in the CFG files.
- The **Category** field is used to logically group similar events for display purposes in HP SIM. These groups are shown when you create event lists and when configuring Automatic Event Handling. This is extremely helpful when wanting to group specific networking, storage, and other traps to be easily found in the user interface. This field corresponds to the *#CATEGORY* keyword in the CFG files.
- The **Enable Trap Handling** field can be toggled to support or suppress events on a per-trap basis. HP recommends that all traps remain Enabled and are only disabled when they are well-understood and can be ignored without any impact. By disabling a specific trap, you are telling HP SIM to ignore that trap once received. If a trap is disabled, then the trap is dropped and not logged in the database. This field corresponds to the *#ENABLE* keyword in the CFG files.

30 Proxy authenticator

HP SIM supports user authentication against the underlying operating system as well as Light Weight Directory Access Protocol (LDAP) server (including Active Directory). However, HP SIM does not support an already existing enterprise SSO solution like Java Open Single Sign On (JOSSO), Central Authentication Service (CAS), Shibboleth, Security Assertion Markup Language (SAML) and so on. By adhering to certain interface requirements of HP SIM, a generic authenticator could be written to meet enterprise SSO needs.



Requirements

OEM clients to provide an authenticator meeting the following requirements:

- To provide HTTP(S) interface
- To accept GET/POST HTTP operation and respond success or failure with XML messages
- To include user name and role (administrator, operator, or user) in the success response

Proxy authenticator additional information

- HP SIM provides a proxy authenticator security module which could be customized using various properties. Some of the properties are configurable only through a property file, `SecuritySettings.props`, found in `SIM_HOME/config` folder, where `SIM_HOME` refers to the location where HP SIM is installed. Some of the property values mentioned in the property file can be overridden at runtime. For more details regarding which properties are mandatory in the property file and which ones could be overridden from URL parameters, please refer to the section [“Settings to be made in HP SIM”](#) (page 163).
- The proxy authenticator creates the user dynamically based on the success response from the Authenticator. Also on every successful response from the authenticator, the role is checked and necessary authorizations will be modified dynamically.
 - The user's authorization is modified if and only if there is a change in the user's role from the previous login (if applicable).
 - The proxy authenticator fails if the user name matches with the default HP SIM administrator (Administrator for Windows and root for Linux and HP-UX).
- The proxy authenticator works only for the Web GUI sign in for HP SIM; however, it can co-exist with the existing form-based authentication mechanisms, wherein a user could login using a username and password.
- Any changes in the `SecuritySettings.props` should be done by the user having Administrator rights; also it requires a restart of the HP SIM service.
- Since the interface requirement is simple - HTTP(S) with XML response, it is assumed that the Administrator is taking into account various network security implications. For example, while

HP SIM allows HTTP as well as HTTPS connections with the authenticator, HP highly recommends you provide support only through certificate-based authentication with the authenticator to avoid any security vulnerability that might arise in the absence of it.

Settings to be made in HP SIM

The following section covers various properties that can be customized to work with Proxy authenticator. Please note that these properties can be configured either once in the property file, or they can be overridden using URL parameters while launching HP SIM.

Serial Number (S/N)	Property	Mandatory In SecuritySettings.props	Override-able Via URL parameter	Default value	Comments
1	isProxyAuth	Yes	No	0	Enable (1) or disable (0) Proxy authenticator Note that a value of 1 indicates that proxy authenticator will be enabled but not enforced. The enforcement is effective if the URL parameter isProxyAuth is also set to 1.
2	proxy.auth.server.trust.check	Yes	No	1	Enable (1) or disable (0) Trust Check This checks if Proxy authenticator is trusted by HP SIM and connect only if it is trusted. Setting this value to 1 is highly recommended to avoid any security vulnerabilities.
3	proxy.auth.keystore	Yes	No	N/A	The full path of the keystore in which the trusted certificates of Proxy authenticator are stored. Note, to avoid security issues, HP recommends that this directory be secured and that the keystore be protected with a strong password.
4	proxy.auth.request.url	Yes	Yes	N/A	The URL of the authenticator where the request will be sent by HP SIM.

Serial Number (S/N)	Property	Mandatory In SecuritySettings.props	Override-able Via URL parameter	Default value	Comments
					HP recommends you ensure this URL is not re-used multiple times, as it might create potential security risks. Also, HP recommends you provide a random token as part of the URL to ensure uniqueness and periodic expiry of the tokens at the authenticator.
5	proxy.auth.request.inputs	Yes	Yes	N/A	A comma separated list of URL request parameters. Note: HP SIM Web GUI to be invoked with these input parameters.
6	proxy.auth.request.method	No	Yes	GET	The HTTP method by which the authenticator will be contacted by HP SIM. The allowed values are GET and POST only.
7	proxy.auth.request.headers	Yes	Yes	N/A	A comma separated list of HTTP request header and value de-limited by a colon. For example, User-agent: HP_SIM
8	proxy.auth.response.success.value	Yes	No	SUCCESS	Value received from Proxy authenticator indicating sign in success.
9	proxy.auth.response.success.value	Yes	No	text/xml	Content-type of response XML data. The response should be XML. text/xml is default Content-type, but if the value is not provided, Content-type will not be validated.
10	proxy.auth.request.connection.timeout	No	No	60000	Connection-timeout for the Proxy

Serial Number (S/N)	Property	Mandatory In SecuritySettings.props	Override-able Via URL parameter	Default value	Comments
					authenticator connection for authentication. These values must be numeric and the value set is considered in milliseconds.
11	proxy.auth.request.socket.timeout	No	No	60000	Socket-timeout for the Proxy authenticator. These values must be numeric and the value set is considered in milliseconds.
12	proxy.auth.response.success.property	Yes	No	N/A	XPath for success value
13	pproxy.auth.response.user.property	Yes	No	N/A	XPath for user name value
14	proxy.auth.response.role.property	Yes	No	N/A	XPath for role value
15	proxy.auth.response.domain.property	No	No	N/A	XPath for domain value
16	proxy.auth.response.name.property	No	No	N/A	XPath for name of user value
17	proxy.auth.response.email.property	No	No	N/A	XPath for email value
18	proxy.auth.response.privilege.property	No	No	N/A	XPath for security modification privilege value. Set 1 for yes and 0 or no value for no.
19	proxy.auth.response.inclusion.range.property	No	No	N/A	XPath for user IP login inclusion range value.
20	proxy.auth.response.exclusion.range.property	No	No	N/A	XPath for user IP login exclusion range value.
21	proxy.auth.client.ipv4.inclusion.range	No	No	N/A	Proxy authenticator will be accessible only from this IP range(s)
22	proxy.auth.client.ipv4.exclusion.range	No	No	N/A	Proxy authenticator will not be accessible from this IP range(s).

Configuring trust check in HP SIM for Proxy authenticator server

Perform the following to enable trust check with the Proxy authenticator:

Procedure 42 Configuring trust check for Proxy authenticator server

1. Create a keystore in a secure folder.
2. Import certificate(s) as trusted certificate(s) in the keystore.
 - a. If the authenticator's certificate is self-signed, import it in the keystore.
 - b. If the authenticator's certificate is CA-signed, import only the CA certificate.
 - c. If the authenticator's certificate is signed by an intermediate CA, then, import all the certificates starting from the root CA to the CA that signed the certificate.
3. Configure `SecuritySettings.props` file to update the keystore specific properties:
 - a. `proxy.auth.server.trust.check=1`
 - b. `proxy.auth.keystore=<full path for the keystore>`
`mypassword -a -x ProxyAuthKeyStorePassword=<password>`
4. Add the keystore password in HP SIM.
Use `mypassword` CLI to set the keystore password. Please note that you need to use `ProxyAuthKeyStorePassword` as the key. For example,
5. Restart HP SIM

NOTE: Use HP SIM's JRE keytool to perform all the tasks related to certificate/keystore. For more details, see <http://docs.oracle.com/javase/6/docs/technotes/tools/windows/keytool.html>

How to use Proxy authenticator

After making necessary configuration changes and restarting HP SIM, the proxy authenticator is automatically enabled if HP SIM is launched, which is the `isProxyAuth` parameter set to 1, as well as passing all of the necessary input parameters as configured in the property file.

For example if the following properties are configured in the `SecuritySettings.props` file:

```
proxy.auth.request.url = https://10.1.2.3/token/@token@
```

```
proxy.auth.request.inputs = token
```

HP SIM is launched using the URL:

<https://10.1.1.1:50000/?isProxyAuth=&token=12398738273127317178127912739731273739127937123719371371893718937197319173>

HP SIM makes a request to the Proxy authenticator using the URL:

<https://10.1.2.3/token/12398738273127317178127912739731273739127937123719371371893718937197319173>

NOTE: Any customization of the URL at runtime is achieved using the pattern “@tag@”, where the special character “@” forms the prefix and suffix and the “tag” represents the incoming URL request variables to HP SIM.

In the above example, 10.1.1.1 is the host running HP SIM and 10.1.2.3 is the host running the authenticator.

Also note that if the value of “proxy.auth.request.url” parameter needs to be overridden by the URL parameter, then launch HP SIM with the complete URL.

<https://10.1.1.1:50000/?isProxyAuth=1&proxy.auth.request.url=https://10.1.2.3/token/12398738273127317178127912739731273739127937123719371371893718937197319173>

A Important Notes

System and object names must be unique

System and object names must be unique in HP SIM.

For example, the name of a Virtual Connect Domain must not be identical to the name of a Virtual Connect Switch, or they can be confused in HP SIM. The Virtual Connect Domain is a virtual system with no physical network address. The Virtual Connect Switch is a physical system that is network addressable.

Setting the Primary DNS Suffix for the CMS

- ❗ **IMPORTANT:** If the Windows server you are installing HP SIM onto is a multi-homed system serving up multiple IP addresses across multiple domains, then it is important that the server has the primary DNS suffix defined for the system. The primary DNS suffix must be displayed in the System Properties as part of the **Full computer name** for the server.
-

In Windows:

Procedure 43 Setting the Primary DNS suffix of the CMS BEFORE installation

1. From the Windows Control Panel, click **System**, and then click **Security**.
2. Click **change settings**. The **System Properties** window appears.
3. On the **Computer Name** tab, click **Change**.
4. The **Computer Name/Domain Changes** window appears.
5. Click **More**. The **DNS Suffix and NETBIOS Computer** window appears.
6. Enter the Primary DNS suffix under **Primary DNS Suffix of this computer**, and click **OK**.

To fix the issue AFTER HP SIM installation, complete the following:

Procedure 44 Deleting duplicate CMS AFTER installation

1. From the command line, run `ipconfig/flushdns`.
2. In the HP SIM UI, on the system view page, select the duplicate CMS system you want to remove.
3. Click **Delete**. If the system cannot be deleted, select the other CMS system and delete it.
4. Select the remaining CMS system, and then select **Options**→**Identify Systems**.
5. Select target systems, and then click **Run Now**.

Distributed Systems Administration Utilities menu options not available

The Distributed Systems Administration Utilities (DSAU) menu items do not work on a HP SIM 6.0 HP-UX CMS. A new version of DSAU will be released to the web in the future.

Virtual machine guest memory reservation size

If HP SIM is installed on a virtual machine guest, but does not start and an empty `mxdomainmgr.0.log` file is observed in the `installation/logs` directory, then use the virtual machine configuration tools to set the guest's memory reservation size to be a minimum of 4GB.

Insight Remote Support Advanced compatibility

- ❗ **IMPORTANT:** If a version prior to A.05.40 of Insight Remote Support Advanced is installed, you must update it to version A.05.40 or higher to preserve configuration information and avoid some manual configuration steps. The latest version of Insight Remote Support Advanced is available at:
<https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=RSADVANCED>
-

Database firewall settings

When using MSDE (or Microsoft SQL Server 2005 Express Edition), Microsoft SQL, or Oracle database server located on a remote Windows XP SP2 server, the firewall settings on the remote server must be turned off. To do this:

1. Select **Start**→**Control Panel**→**Windows Firewall**.
2. Click **Turn Windows Firewall on or off**.

Annotating the portal UI

Annotation refers to adding a small amount of textual information, such as the name of the Central Management Server (CMS), near the product name when browsing to the CMS. Areas that can be annotated are the browser's title bar, the sign-in page, and the banner. Annotation is supported by adding values to `globalsettings.props` entries whose names are:

```
ANNOTATION_SIGN_IN_PAGE_HTML  
ANNOTATION_BANNER_HTML  
ANNOTATION_BROWSER_TITLE_TEXT
```

The names all begin with `ANNOTATION` so that they sort together and are easy to find. They end with `_HTML` or `_TEXT` to indicate how the value is treated as HTML or text. Note that simple text is valid HTML.

Browser title annotation uses `ANNOTATION_BROWSER_TITLE_TEXT`:

- The annotation is appended to the product name in the browser title.
- The annotation is treated as text.
- The annotation is prepended with a space.

Sign-in page annotation uses `ANNOTATION_SIGN_IN_PAGE_HTML`:

- The annotation is put below the product name.
- The annotation is treated as HTML.
- The annotation uses the same style (font, font size, and so on) as the product name but can be modified by using HTML in the annotation.

Banner annotation uses `ANNOTATION_BANNER_HTML`:

- The annotation is appended to the product name in the banner of the portal.
- The annotation is prepended with a space, for both maximized and normal portal states.
- The annotation uses the same style (font, font size, etc.) as the product name but can be modified by using HTML in the annotation.

The `globalsettings.props` file is a text file that can be manually edited. It is located at:

- On Windows: It is typically located at `C:\Program Files\HP\System Insight Manager\config\globalsettings.props`.
- On HP-UX and Linux: It is located at `/etc/opt/mx/config/globalsettings.props`.

Alternatively, when setting simple values, the `mxglobalsettings` command line utility can be used. The following is an example of setting simple values from the command line:

```
mxglobalsettings -s ANNOTATION_SIGN_IN_PAGE_HTML=alwayson.company.com  
mxglobalsettings -s "ANNOTATION_BANNER_HTML=- alwayson.company.com"  
mxglobalsettings -s "ANNOTATION_BROWSER_TITLE_TEXT=- alwayson.company.com"
```

Security bulletins

HP software products contain multiple third-party components, such as OpenSSL. HP discloses that the non-HP owned software components listed in the **Systems Insight Manager** end user license agreement (EULA) are included with **Systems Insight Manager**.

To view the EULA, use a text editor to open the `eula_license.xml` file, and search for **third-party software**.

HP addresses security bulletins for the software components listed in the EULA with the same level of support afforded HP products. HP is committed to reducing security defects and helping you mitigate the risks associated with security defects when they do occur.

HP has a well defined process when a security defect is found that culminates with the publication of a security bulletin. The security bulletin provides you with a high level description of the problem and explains how to mitigate the security defect.

Procedure 45 Subscribing to security bulletins

1. Open a browser to the HP home page:
<http://www.hp.com>
2. Click the **Support & Drivers** tab.
3. Click **Sign up: driver, support, & security alerts**, which appears under **Additional Resources** in the right navigation pane.
4. Select **Business & IT Professionals** to open the Subscriber's Choice web page.
5. Do one of the following:
 - Sign in if you are a registered customer.
 - Enter your email address to sign-up now. Select **Driver and Support alerts** and click **Continue**.

Validating RPM signatures

The RPMs for HP SIM for Linux are digitally signed with HP's official private key. You can use the `rpm-hpPublicKey.pub` provided with the HP SIM's Linux distribution or go to the official HP website to download HP's public code signing key.

Checking which public keys are installed

Check which public keys are installed on your system with the following command:

```
# rpm -q grep-pubkey
```

Where `grep-pubkey` finds all the public keys installed on the system.

Alternatively, you can use the `rpm -qi` command to show more details about the certificates.

The following procedure installs HP's code signing public key.

```
# rpm --import rpm-hpPublicKey.pub
```

Validate the signature on an RPM

Use the `rpm -checksig` command to validate and verify the digital signature of an RPM. The output from the command indicates whether or not the RPM is correctly signed, as shown in the example below:

```
# rpm --checksig <hpsimrpm>
```

How to check RPM signatures within the sysmgmt.bin

To check RPM signatures in the `sysmgmt.bin` before installing HP SIM, complete the following procedure:

```
chmod u+x sysmgmt.bin
./sysmgmt.bin --keep --confirm
(and type y to extract the archive and n to execute
./mxbundle.server.postinstall)
```

This creates a temporary directory. For example, `makeself-32350-20091024210345`, is where the HP SIM RPMs will be located. You can use the `rpm --checksig` command to verify the HP signature of the RPMs. After verifying the RPM, enter `./sysmgmt.bin` to install HP SIM.

If you install HP SIM `sysmgmt.bin` without installing the HP public key, you will receive the following warning:

```
Installing hpsim* ...  
warning: hpsim-C.06.00.00.00.%20091027-1.i386.rpm: V3 DSA signature: NOKEY, key ID 2689b887
```

Central Management Server

Resource-intensive applications such as HP Insight Control performance management have sometimes encountered problems working with large numbers of systems. In an effort to improve the stability of the CMS, HP SIM imposes a limit of 2000 systems on the information that is provided to these applications. This limit can be changed, if necessary, by adding a new property named `MaxNodesViaSOAP` to `globalsettings.props` and setting it to the desired number of systems. Setting `MaxNodesViaSOAP` to a negative number disables the limit checking. In some cases, setting this limit to a number greater than 2,000, or disabling the limit, can result in errors, including the possibility of HP SIM hanging or crashing.

Installing the CMS on Windows uses the user desktop locale to determine the CMS locale. For example, if you install the CMS on a German Windows system and the user desktop locale happens to be English, then the CMS installed becomes an English CMS.

The language of `mxlog.txt` (a log file) currently depends on the CMS locale. If the installer user desktop locale is German, `mxlog.txt` is logged in German, even though the CMS is installed on an English Windows system and the browser locale is also English.

This happens because the `Log On As` property of the HP SIM service is configured as the install user name, instead of `Local System`, which specifies system environment. Running the service with the credentials of the user that installed the application is necessary for the service to have the necessary credentials for database access and other CMS settings.

If you want the logs to be in a different language (German or English), you have three options:

- Stop HP SIM service. Change the default locale of the user account specified in the `Log On As` property of the HP SIM service (the user that performed the install) to the desired language, and restart the service.
- Stop HP SIM service. Change the `Log On As` user for the HP SIM service to the local administrator account, and be sure its locale is set to the desired language. Restart the service.
- If you do not want to change the default locale of either of the previous accounts to the desired language for the logs, create a new administrator-level account with the desired default locale. Then uninstall HP SIM and reinstall HP SIM specifying the new administrator-level account.

On a Windows NT 4.0 system running Internet Explorer 6 Service Pack 1, remotely browsing into a CMS causes a DLL failure after being connected for hours. This issue occurs on a Windows CMS and on an HP-UX CMS.

Complex systems displaying inconsistency with the number of nPars within the complex

When viewing the complex through the **System Page** or Report, the number of nPars represent the total number of nPars that can potentially be in the complex, regardless of the state of the individual nPars. Alternatively, when viewing nPars within a complex under a system collection, the number of nPars associated with a complex is equal to what HP SIM has determined through a WBEM provider. Therefore, the number of nPars shown in the system collection might be less than or equal to the number displayed in the **System Page** or Report.

Configure or Repair Agents

Configure or Repair Agents tasks that combine Critical, Unknown, and Unmanaged targeted systems appear to hang at 0% but will eventually complete.

Data collection reports

Data Collection reports might report the network interface for HP-UX systems incorrectly. This is due to an issue with SNMP agents on HP-UX. In the future, the HP-UX WBEM provider will include a Link Aggregate Provider to report the network interface on HP-UX systems, and HP SIM can then provide the correct data from the WBEM provider.

B Troubleshooting

Adobe

HP recommends you use Adobe 11.

Agentless Management Service

HP Agentless Management Service may exhibit slow performance on SLES 10 if the latest HP iLO Channel Interface driver is not installed on HP ProLiantGen8 servers. HP recommends you upgrade SLES10 HP iLO Channel Interface driver to V1.2 or later.

AMS re-installation through Configure or Repair Agents on an RHEL 6.2 target might fail, even though the force install option is selected. Uninstall AMS from target and then install through Configure or Repair Agents, it will install it successfully.

Authentication

SSH key authentication is not configured when a system is discovered for the first time.

SSH configuration for Linux and HP-UX systems:

Procedure 46 SSH configuration for Linux and HP-UX systems

1. On the HP-UX system being managed, edit the following file:

`/opt/ssh/etc/sshd_config`

On the Linux system being managed, edit the following file:

`/etc/ssh/sshd_config~`

2. Search for the following line:
`KerberosAuthentication yes`
3. Edit the line as follows:
`KerberosAuthentication no`
4. Restart the sshd process.

On a Linux or ESX system, you might receive the following error when running the `mxagentconfig` command or through Configure or Repair Agents:

Configuration failed to complete due to the following exception: Could not access the file or directory `sshd_config.orig` on the target system `esxhost1`. Remote system reported following error message: Permission denied. Check whether the directory or file exists or whether the user has the operating system permission to access it.

Solution: You must manually change the permissions in the file to 644.

Blade insertion

When a Blade is inserted in to an enclosure, Onboard Administrator will notify HP SIM about this event through a Blade Insertion Trap. In order to synchronize the topology of the Enclosure within HP SIM, upon reception of Blade Insertion trap HP SIM triggers reidentification on the Onboard Administrator. Since this operation is triggered immediately upon trap reception, it was observed that at times the Onboard Administrator is still not ready with the latest updated information. This results in an error message in HP SIM that the Onboard Administrator XML is incomplete which is raised as an event and can be seen from **All Events** in HP SIM.

To work around this issue, reinitiate identification on the Onboard Administrator after waiting for a moment. Live lab tests have shown that, after waiting for 60 seconds (one minute), the information

in Onboard Administrator is refreshed. The time taken could be lesser than this at times, but 60 seconds is a conservative time interval which could be relied upon.

In HP SIM 7.2, upon reception of Blade insertion trap from Onboard Administrator, rather than immediately kicking off reidentification HP SIM waits for a configurable interval of time and then initiates re identification. The configurable parameter is *bladeInsertDiscoveryWaitTime*. This parameter is a global setting and is currently configured to 60 seconds. For all practical purposes this interval is sufficient. However if there is a case due to slow responding systems, if this interval is found to be insufficient, then you can change the default value through the command line interface: go to <sim_install_dir> and execute the following command: **mxglobalsettings -s bladeInsertDiscoveryWaitTime=120**, where 120 represents the new value in seconds.

Browser

If you are using a Firefox browser, you should avoid remaining on the **Task Results** page for an extended period of time. If you notice the browser becoming sluggish while viewing the **Task Results** page, you should sign out of HP SIM to allow the browser to release memory. You can then sign back in.

My Browser is displaying an error message Communication with the HP SIM server has been lost.

Solution: The HP SIM portal relies on the CMS to respond quickly to all requests.

- If the CMS is slow to respond to one request, browser performance can fall significantly during that time.
- If the CMS is slow to respond to two requests, the browser appears to lock up completely during subsequent interaction; the browser does not send additional requests until there are fewer than two outstanding requests.
- If four sequential ping-like requests takes more than 30 seconds each to complete, either due to request queuing or slow CMS response, the browser displays the message, Communication with the HP SIM server has been lost, even though the CMS might still be responsive to other browser sessions.

By default, web browsers are limited to two simultaneous connections to a single web server. If two requests are outstanding, any additional requests wait until one of the current connections completes. This is by design and is in agreement with the HTTP 1.1 specification. The HP SIM UI generates many requests, many of them simultaneously. The HP SIM portal relies on the CMS to respond quickly to all requests. On a LAN, the browser receives a CMS response to most requests within 10 to 100 milliseconds, which is nearly instantaneous. Requests that involve database queries or secondary network communication might take a few seconds to respond. The following situations might result in particularly slow response times:

- Viewing large collections of systems or events.
- Specific or custom database queries taking an unexpectedly long time.
- Many users simultaneously accessing a shared resource, such as the database.
- Pages (for example, System Properties) that retrieve data using WBEM or SNMP and display the results, especially when the requests are destined to time out.

Solution: The maximum number of server connections can be increased in both Internet Explorer and Firefox. The default number of connections is two. Though you can increase this number into the hundreds, it's recommended not to exceed ten. For more information, see:

- Internet Explorer: <http://support.microsoft.com/kb/282402/>
- Firefox: <http://kb.mozillazine.org/Network.http.max-persistent-connections-per-server>

When browsing to HP SIM using Microsoft Internet Explorer 6.0.3790.0 on Windows 2003, the billboard in lower corner of the **Home** page is blank.

Solution: Enable **Play Animations in Web Pages** in Internet Explorer. To access this, select **Tools→Internet Options→Advanced**, and then select **Play Animations in Web Pages** under the **Multimedia** section.

If you receive a Page Not Found browser error when launching HP Insight Control performance management tools from within HP SIM, the CMS name link might not have resolved correctly on the network.

Solution: Note the name being used in the browser window, verify that the name resolves on the network, and that it is not being affected by any proxy settings in the browser.

When you try to browse to the HP SMH on the same Linux system that HP SIM is installed, you might receive multiple browser warning messages.

Solution: Complete the following:

1. Open a terminal window.
2. At the command prompt, enter: `/etc/opt/hp/hpsmh/certs /opt/hp/hpsmh/certs`
3. Press the **Enter** key.
4. At the command prompt, enter: `service hashed restart`
5. Press the **Enter** key.

Central Management Server

Resource-intensive applications such as HP Insight Control performance management have sometimes encountered problems working with large numbers of systems. In an effort to improve the stability of the CMS, HP SIM now imposes a limit of 2000 systems on the information that is provided to these applications. This limit can be changed, if necessary, by adding a new property named *MaxNodesViaSOAP* to `globalsettings.props` and setting it to the desired number of systems. Setting *MaxNodesViaSOAP* to a negative number disables the limit checking. In some cases, setting this limit to a number greater than 2,000, or disabling the limit, can result in errors, including the possibility of HP SIM hanging or crashing.

When you cannot access HP SIM on a Windows system using a full DNS host name, your Windows DNS; configuration is not set properly.

Solution: There are several reasons and workarounds for this:

- **The TCP/IP Settings for your Network Connection are not configured properly.**
HP recommends the following workaround:
 1. On the CMS, open the Control Panel, and select **Network Connections→Local Area Connection Settings→Internet Protocol (TCP/IP)→Properties→Advanced**.
 2. Select the **DNS** tab.
 3. Be sure that DNS suffix for this connection contains the full DNS suffix for the system.
 4. Be sure both the **Register this connection's address in DNS** and the **Use this connection's DNS suffix in DNS registration** checkboxes are selected.
- **The System name for the CMS is not configured properly.**
HP recommends the following workaround:
 1. On the CMS, open the Control Panel and select **System**.
 2. Click **Network Identification**.
 3. Click **Properties** or **Change** next to the **Rename this computer or Join a domain** field.
 4. In the dialog box, click **More**.
 5. Be sure the primary DNS suffix is set correctly. If not, set it, and click **OK** until all dialog boxes are closed.
- **The proxy settings on the client browser is configured to proxy local systems.**
HP recommends the following workaround:

1. In Internet Explorer, select **Tools**→**Internet Options**→**Connections**→**LAN Settings** and then select **Use a proxy server for your LAN**.
 2. Click **Advanced**.
 3. Add the DNS suffix for the CMS to the **Exceptions** list.
 4. Click **OK** until all dialog boxes are closed.
- **The company DNS servers could be having problems.**
HP recommends that you contact your company's network support group.

Complex

You cannot delete a complex and all associated systems when you first select either the system or complex alone and then try to delete.

Solution: You must select all associated systems from the list for the deletion to work correctly.

Configure or Repair Agents

If you are unable to configure VCA using credentials, go to **Tools**→**Protocol Settings**→**Global Protocol Settings** or **Options**→**Discovery**→**Configure Global Protocol Settings**, and change the http Settings: Default read timeout (seconds) to 25 or more.

Configure or Repair Agents fails for a managed system having Windows operating system and OpenSSH 5.4 p1-1 or greater.

HP SIM 7.2 ships a new version of OpenSSH. This version of OpenSSH considers credentials as case sensitive, resulting in an authentication failure if credentials are not provided in proper case. Therefore, you must provide case sensitive Sign-In credentials during discovery or while running the Configure or Repair Agents task.

For example: Some Windows managed systems have the username as 'Administrator'. During discovery the Sign-In credential username is provided as 'administrator', then, Discovery and few other tasks will work perfectly because Windows does not consider credentials as case sensitive. However, the Configure or Repair Agents task fails because OpenSSH considers 'Administrator' and 'administrator' as different users.

To resolve this issue, you can complete one of the following:

- Update the Sign-In credentials with proper case. (Recommended)
- or
- Do not use Sign-In credentials and provide credentials (with proper case) manually before running the Configure or Repair Agents task.

When configuring agents from a Linux or HP-UX CMS on a Windows system, you may receive an STDERR error. The content that is coming on the STDERR console in HP SIM, is captured from the error stream of the process which is created during the configuration on the target system. The contents of the standard error stream depends on the operating system of the CMS and the operating system of the target system. The same content can be seen when you manually run the command on the CMS for the target system.

If you see the error on the STDERR console in HP SIM, there is nothing wrong going on in the background. HP SIM displays the content of both the output and error streams.

When you try to do any configuration from a Linux CMS to a Windows 2012 server, ensure the CMS has a in-built SMB server 3.0. If the CMS has any prior version of SMB server installed, then internal commands like `put` etc will fail. As a result, the CMS cannot copy the configuration files to the windows 2012 server node. Therefore, the Configure or Repair Agents task will fail.

NOTE: Windows server 2012 uses SMB 3.0(or SMB3) on the file server. Windows Server 2012 Hyper-V only supports SMB 3.0 for remote file storage.

The Remote Registry service is not started by default on the workstations like windows7 and Windows Vista. If this service is not started, then Configure or Repair Agents on these target systems will fail.

To start the service, follow the steps below:

Procedure 47 Starting Remote Registry service

1. Enter `services.msc` in run. This displays the list of services.
2. Select the Remote Registry Service and start it and also change the startup type to Automatic.

Configure or Repair Agents cannot be used to install the WBEM Providers to Integrity Windows systems.

You must manually install the WBEM provider by copying `cp010621.exe` (can be found in the `smartcomponents` directory under the HP SIM install) to the target system and then running it.

HP-UX 11.31 does not ship with `smbclient`, therefore, any Configure or Repair Agents task from an HP-UX 11.31 CMS to a Windows target fails until `smbclient` is installed on the CMS.

Solution: A back up `smbclient` is located under `/opt/mx/bin/smbclient`. Copy this to the `opt/samba/bin/smbclient` folder to execute the Configure or Repair Agents task.

How do I push an SSH key using `mxagentconfig` to a target system running Windows Vista?

Solution: HP recommends turning off the Windows Vista User Account Control.

How do I push an SSH key through Configure or Repair Agents on Windows 2008?

Solution: HP recommends disabling User Account Control on Windows 2008 systems.

NOTE: Configure or Repair Agents is not supported on Windows Vista.

I received a connection failed error in Configure or Repair Agents on Windows XP.

Solution: You might have Windows XP SP2 or later installed. Windows XP SP2 disables admin share. You must enable admin share by using the command `net share admin$`.

Container View

When the SNMP protocol is disabled and the WBEM protocol is enabled, the HP Integrated Lights-Out (iLO) firmware version is displayed as **Not Available** in tool tip of the Picture View.

Solution: To view the iLO firmware version, enable the SNMP protocol. To do so, select **Options**→**Protocol Settings**→**Global Protocol Settings**.

Solution: This can happen when the enclosure contains at least one double dense blade (BL2x220c or ProLiant xw2x220c Blade Workstation) and all the slots in the enclosure are populated with the servers. A double dense blade contains 2 servers per blade: an A and a B server. Some of the cases where the number of servers exceeds the available slots in the enclosure are:

C7000 containing 15 BL servers (single sided) and 1 Double dense server = 17 servers

C7000 containing 10 Double dense servers = 20 servers

Therefore with number of servers exceeding the number of available slots, the B side of each blade beyond the 8th double dense blade or beyond the 16th blade will be missing from HP SIM. The servers can still be discovered, but they will not be associated with the enclosure or will not be shown in enclosure container view

The table view of a rack appears empty but the container view has a rack diagram.

Solution: This error can happen if you unplug the power supply and then plug it back in. Therefore, you must re-run discovery.

HP ProLiant BL e-Class blade servers or the HP bc1000 blade PC container view is empty but the table view displays all blades correctly.

Solution: This happens when the Integrated Administrator is discovered before blades are discovered. Therefore, run identification on the Integrated Administrator management processor.

1. Select **Options**→**Identify Systems**.
2. Select the ProLiant BL e-Class Integrated Administrator.
3. Click **Run Now**.

Credentials

If you have problems where credentials are not being saved in HP SIM on a Firefox system, HP recommends you use latest version available of Firefox. Reference:

<http://support.mozilla.org/en-US/questions/919779>

<http://support.mozilla.org/en-US/questions/922291>

When more than one credential is not specified on the **Edit System Credentials** page, ESXi 5.0 will be discovered with multiple WBEM credentials.

- If an ESX system is in lock down mode enabled, Sign-In and WBEM credentials will be masked on the **System Credentials** page.
- If an ESX system is in lock down mode enabled, Sign-In and WBEM credentials will be masked under view all **System Credentials** page.
- If an ESX system is in lock down mode enabled, Sign-In and WBEM credentials will be disabled for editing on the **System Credentials** page..

For HP SIM to set the sign-in credentials for a system after successful discovery, be sure the following settings are made:

- If the system that is being discovered only supports WBEM/WMI protocols apart from SNMP; for example, Windows systems, then for HP SIM to set Sign-in credentials, enter the WBEM/WMI credentials under the **Sign-in** credentials tab. Do not enter the credentials under the **WBEM/WMI** credentials tab in the discovery task.
- If the system that is being discovered supports multiple protocols apart from SNMP, like WBEM and SSH, be sure either the SSH or WBEM credentials are entered under the **Sign-in** credentials tab in the discovery task.

If you delete a credential (system credential, global credential, or one configured with a discovery task) while discovery or identification is running, and that credential is found to work with a system, the attempt to write the working credential to the database fails because the original credential has been removed. If you try to view System Credentials for such a system, the system will not be listed in the **Credentials that are in use** table, or the table includes `No data available`. Normally, a system is listed in this table; even one with no working credentials is listed with an Access Type of None.

To resolve this issue, restart HP SIM to remove any extraneous database records, and re-run the discovery or identification task.

Data Collection

Capacity information is not available from providers for passively managed storage arrays.

If you have more than 2000 objects in an array, you must increase the default data collection time to 32400, by modifying the `Storage_DC_Timeout` field in the `globalsettings.props` file.

When the number of objects to be collected on any given storage array exceeds 1000, it is possible that data collection will fail for the array with a default timeout value of 10800 seconds.

After a HP SIM upgrade, the Data Collection task might fail when executed.

Solution: Following upgrade procedures, you must run either the Identification Task or System Discovery Task against the systems for them to be reconciled following the completed upgrade procedure. The Daily Identification task is available by default and can be ran be any time by selecting **Run Now**. In a future release, the upgrade process will incorporate the automatic launching of the Identification task against discovered systems.

The Data Collection task for an Onboard Administrator times out on non-Windows CMS.

Solution: This affects the individual task only and does not affect other tasks in the batch.

HP SIM might report duplicate entries for array controllers if the data is collected using both WBEM and SNMP protocols on a HP Insight Management WBEM Providers for Windows Server 2003/2008 target.

Solution: To see the correct data in report, you can perform data collection by disabling one of the protocols. You can also access HP SMH to see the correct number of array controllers.

You see a problem with more than two `mxinventory` processes starting on the CMS.

Solution: Complete the following:

Procedure 48 Issue with two `mxinventory` processes starting

1. Verify that your HP-UX CMS has the latest HP-UX kernel patches required for Java 1.5 execution. If the CMS is HP-UX 11.23 IA/PA, then verify that the PHKL_35029 Kernel patch (or its superseding patch) is installed. See <http://www.hp.com/go/java>.
 2. Verify that all your HP-UX managed systems have HP WBEM Services for HP-UX A.02.00.11 or newer and for managed systems running HP-UX 11.23 IA/PA, verify the PHSS_33349 Kernel path (or its superseding patch) is installed.
-

If you cancel a running task, by clicking **Stop** or **Delete**, and immediately try to start another task of the same type, the second task does not run until the previously canceled task fully completes the cancellation. Systems in the cancelled task that are currently being processed are allowed to run to completion. For some long-running tasks like data collection or software deployment, it can take some time to allow the systems in progress to reach completion and finally cancel the task.

Solution: If data collection runs for an unusually long time you might want to stop or delete the task, and wait 5 to 10 minutes after the cancellation has completed before running another data collection task.

If the data collection task is allowed to run to full completion without canceling, another data collection task cannot be run for at least 15 minutes or the task will fail because it is skipped (this would be shown in the STDOUT of the task instance).

If you see that data collection failed because of a WBEM connection, it might be caused by a failed WMI Mapper proxy.

Solution: Complete the following steps:

Procedure 49 Issue with data collection failing because of WBEM connection

1. Physically verify all of the configured Pegasus WMI Mapper proxies. From the **Administrative tools**→**Services** menu on the server hosting the Pegasus WMI Mapper proxy, be sure the Pegasus WMI Mapper is running.
2. If not, restart the Pegasus WMI Mapper if possible.

3. If you are unable to restart the proxy or if the Pegasus WMI Mapper was uninstalled, delete it from the CMS WMI Mapper Proxy settings found in the **Options→Protocol Settings→WMI Mapper Proxy** page.
4. Be sure you have at least one running Pegasus WMI Mapper Proxy configured in HP SIM.
5. Verify credentials for the systems.
6. Run identification on all systems.

If data collection of a system fails with the STDOUT error, stating An error occurred connecting to this system with the WBEM protocol. Check the system configuration

Solution: This might be caused by any of the following conditions:

- You failed to make appropriate port number entries in the `wbemportlist.xml` file:
On Linux and HP-UX: `/etc/opt/mx/config/identification`
On Windows: `C:\program files\hp\systems insight manager\config\identification`
The folders listed above are the default folders and should be used unless you have changed the installation folder location.
- You might have failed to set up and specify appropriate WMI Mapper proxy servers.
- You might have failed to specify appropriate WBEM credentials.

If you run a data collection task on a storage host and select the **Append new data set (for historical trend analysis)** option instead of the default option, **Overwrite existing data set (for detailed analysis)**, the data collection task will fail and the data for that storage host is erased.

Solution: To restore the missing data, do one of the following:

Procedure 50 Issue with data collection failing and data for the storage host being erased

1. Delete the storage host from the HP SIM database, and then discover it again.
2. Wait fifteen minutes, and run the data collection task again with **Overwrite existing data set (for detailed analysis)** selected.

Database

Database creation under SuSE 10 PostgreSQL reports warning messages at various stages as the database is created.

Solution: A warning message states that the view which provides license reporting has caused an exception and has not been inserted. Subsequently, there are warnings indicating that the license view cannot be dropped as it does not exist (creation failed earlier). However, the final step for updating the database in HP SIM 5.1 or later correctly inserts the license view for SuSE 10. Therefore, the view is present when database creation is complete and license reporting should function correctly.

Discovery

Whenever a system in a domain is removed from the domain, by joining it to work group and by removing all DNS entries in DNS Server, the network name retains full FQDN in HP SIM, even after triggering multiple identifications and by discovery with local account credentials again. If you retain the Network Name, verify if the DNS is down. If the system is not down, verify the DNS entries for that system. Then, update the Network Name in the HP SIM UI.

A managed system must not have Hyper-V host, SMI-S Storage CIMOM proxy, and SCVMM installed together. If they are all installed, HP SIM will not be able to set all the subtypes.

To discover an XP P9500 array, you can either discover it with a CVAE server or discover it with embedded SMI-S. Do not use both methods of discovery together because there are chances for Data collection and WBEM subscriptions to fail. However, if you use both methods of discovery and observe that Data Collection or WBEM subscription is failing please delete the system and run discovery again.

Discovery of a Microsoft Windows 2008 MSCS cluster in HP SIM fails to illustrate the second IP address on the **Cluster Monitor** page even though HP SIM discovers the cluster correctly.

Solution: If the first IP address of the MSCS cluster is not in the same subnet as the HP SIM server, a pop-up window appears when browsing to the **Cluster Monitor** page. See the Microsoft link for setting up MSCS cluster with two-subnet Failover Cluster at <http://technet.microsoft.com/en-us/library/bb676403.aspx>.

For Windows 2008 MSCS clusters (including Hyper-V clusters), DHCP addresses are now allowed for the cluster alias. In some circumstances the reverse lookup for the cluster alias IP resolves back to one of the cluster nodes instead of the cluster alias name.

Solution: If this occurs, HP SIM will not add the cluster and the cluster nodes will not be associated in HP SIM with the cluster. To work around this, add an entry to the hosts file on the HP SIM server for the cluster alias name and IP. On Windows, the host file is located in the %windir%/system32/drivers/etc directory. The standard hosts file entry should be of the following form: IP Hostname alias (for example: 15.2.9.1 hypc11.vse.adapps.hp.com hypvc11).

Discovery of an MSCS cluster service name or IP address (for example. a Fileserver service, and so on) overwrites MSCS system information, making management of the cluster nodes through HP SIM, HP Insight Control virtual machine management, or HP Insight Dynamics impossible.

Solution: Remove all systems associated with the MSCS cluster (this includes the cluster alias, the cluster nodes, and any VMs that might be running on the cluster), and then re-discover the cluster (and any VMs) without discovering the service. For example, add the IP address of the cluster service to the ping exclusion range on the general discovery settings page.

When the number of objects to be collected on any given storage array exceeds the value of ~2500, it is possible that data collection will fail for the array.

Solution: This is due to a default timeout value of three hours for this operation. There are two ways to resolve the issue:

- Configure the array to have a maximum of 2500 collectible objects (volumes, disks, ports, and so on).
- Increase the timeout value, depending on the configuration, to an optimal value by modifying the configurable parameter *Storage_DC_Timeout* which is set to a default value of 10800 (equals 3 hours), with the `mxglobalsettings` command.
 - Example to retrieve the current value:
`mxglobalsettings -ld Storage_DC_Timeout`
 - Example to modify the value to 4 hours (14,400 seconds):
`mxglobalsettings -s Storage_DC_Timeout=14400`

It has been observed that data collection can take 3 hours and 37 minutes on an XP24000 array that has ~3200 drives, 40n network ports, and ~150 disks.

If an HP Logical Server that is created in Insight Dynamics is given the same name as the operating system host name of the blade on which it is applied, then the logical server is deleted when the blade is rediscovered.

Solution: To avoid this, be sure the logical server name is different from the host name of the blade.

If you:

- Configure an HP Serviceguard package as an HP virtual machine which is hosted by two different HP virtual machine hosts,
AND
- Complete a failover of the package from one HP virtual machine host to the other one,
AND
- Re-identify the package in HP SIM,

you might find that the package is not associated with the correct HP virtual machine host.

Solution After a Serviceguard package fails over from one host to a different host, you must re-identify the HP virtual machine host system in HP SIM to see the correct association.

Orphan systems are appearing after I run discovery.

Solution: To prevent orphans from appearing in the future, review events and remove the system that you have migrated to a new system type before rediscovering the new system after it is booted. This is true of systems moving in or out of a virtual system environment.

If you see the preferred system name is different than the host name of the full DNS name for an HP virtual machine guest, it is because the preferred system name is specified in the virtual machine package.

Solution: If you want HP SIM to display the same name as the host name of the full DNS name, you must use the `modify` command to modify it.

If an iLO or Onboard Administrator was discovered prior to enabling/configuring Single Sign-on (SSO), re-identification is required for SSO communication to work between HP SIM and the iLO/OA.

If an Onboard Administrator is discovered with **Discover systems in an enclosure when Onboard Administrator is discovered** option enabled, then the percentage completion of the discovery task in which the Onboard Administrator IP address is part of, fluctuates. Initially, the percentage completion is higher, but as the discovery of iLOs are triggered, the overall percentage completion comes down. As the iLO discovery completes, the percentage completion moves higher and finally becomes 100% and task status becomes complete.

Some systems, such as Cisco Fibre Channel switches, that support both SNMP and SMI-S protocols can appear as two separate systems within HP SIM.

HP SIM currently does not support an association of management processor to server if the system is based on PA-RISC because a management processor is only supported on HP Integrity systems. This will not be supported until a new release of firmware for the PA-RISC systems.

If the partition has a vPar already created and been discovered by HP SIM but the IP address used by the vPar has been moved to a stand-alone server, HP SIM will not delete the association to the complex or the management processor; the reason is the partition still has vPar defined within the partition.

If after discovery runs, you can see the CMS, but not the iLO associated with it, check the following:

- Be sure both the IP of the CMS and the iLO are discovered.
- Be sure to enter the iLO credentials on the **Options→Security→Credentials→Global Credentials**. After setting the credentials, rerun discovery.
- Run Configure or Repair Agents to be sure SNMP is configured on iLO and set correctly at the CMS.

Deployment to an iLO with Trust Platform Module (TPM) enabled on the server will fail. You can only deploy iLO firmware if TPM is disabled.

Linux servers

When a Linux server is discovered as an unmanaged system:

1. Be sure to make the changes similar to the following in the `/etc/hosts` file on the discovered system before installing agents:

```
#Do not remove the following line, or various programs
#that require network functionality will fail.
127.0.0.1 localhost
172.24.30.34 HPSIM.wbemqa.com HPSIM
```

Note: Replace the IP address, host name, and alias previously listed with your localhost IP address, DNS name, and host name.

2. Install agents.
3. Verify that the following lines are entered in the `/etc/snmp/snmpd.conf` file. If not, stop the SNMP service, enter them manually, and restart the SNMP service.

```
rwcommunity private
rocommunity public
```

Note: The community strings used should match those community strings on the CMS.

After completing these steps, the system is discovered properly.

To discover detailed information for Linux running on ProLiant systems, you can do one of the following:

- Install the Linux ProLiant agents on the system.
- Update the `snmpd.conf` file. If you choose this option and do not update the `snmpd.conf` file, LINUX appears in the **Operating system name** column on the system table view page, instead of the true operating system name, such as Red Hat Advanced Server.

To solve this issue:

1. Stop the SNMP daemon.
2. Add the following line to the `/etc/snmp/snmpd.conf` file:


```
rocommunity public
```
3. Restart SNMP.

Enclosure table view page

iLO's do not appear in the enclosure table view page. However, to access the iLO from this view, click the status icon in the **MP** column of the associated server.

Event

When you subscribe for WBEM events from either the command line (`mxwbemsub`) or the GUI (**Options→Events→Subscribe to WBEM Events**), you might receive the error message `String index out of range`.

Solution: Verify if the name of the local host resolves to a fully qualified name through DNS. The command needs the FQDN name to work properly.

To enable non-administrative users to delete or clear events, you can create a toolbox with the **Clear Events** and **Delete Events** tools.

1. Select **Options**→**Security**→**Users and Authorizations**.
2. Click the **Toolboxes** tab and click **New**
3. In the **Name** field, enter a name for the new toolbox.
4. In the **Description** field, enter a description for the new toolbox.
5. **Select Toolbox** is enabled.
6. Under **Show Tools in Category**, select **Configuration Tool** from the dropdown list.
7. Select **Delete Events** and **Clear Events**, and move them to the **Toolbox contents** window.
8. Click **OK**

Next, create an authorization on the systems that you want to enable the user to clear or delete events.

1. Select **Options**→**Security**→**Users and Authorizations**.
2. Select the **Authorizations** tab, and click **New**.
3. In the **Select** field, select the users or user groups to which to assign the toolbox.
4. In the **Select Toolbox(es)** section, select the toolbox you created in step 2.
5. In the **Select Systems** section, select the systems that you want this toolbox to apply.
6. Click **OK**.

Create an event collection, and run the tool through the menus.

When event types are dynamically added, you must manually refresh any event collections that are currently displayed

Health status

While viewing MSA G3 health status on system page.

1. When any of the array's sub-component is in non-ok status, the status of the `TopComputerSystem` will also be set to non-ok status. It is not necessary that both these statuses have same value. For example, when a Vdisk is in Offline status, the operational status property of this vdisk is set to "15", and the `TopComputerSystem`'s operational property value is set to "3" (Degraded).
2. Currently HP has implemented the `GroupSystemSpecificCollection` class for some components like Controllers, Vdisk, Temp.Sensors, Fan and Power Supply. When the Overall health status is non-ok and none of these `GroupCollection` instances is in non-ok status, this means the faulty component is not covered by these collection instances.

Host name

When installing HP SIM, CMS host names that exceed 15 characters are truncated, and the truncated name must be used to complete the installation. After the install, two administrator accounts are created. One account includes the *original hostname\administrator* and the other account includes the *truncated hostname\administrator*.

Solution: To sign in, you must use the original host name in the **Domain** field on the **Sign in** page.

HP Insight Control power management

To manage ProLiant blades running ESX 3.0.x or 3.5 with the virtual ID option turned on, the HP ProLiant SNMP Agent for ESX package must be installed. You can use the Configure or Repair Agents feature in HP SIM to install the package. If you have already discovered ESX classic servers before the ProLiant SNMP Agent is installed, you must delete these systems, install the ProLiant SNMP agent on them, and re-discover them.

While restoring the Onboard Administrator configuration, initially the following message appears if the network communication to Onboard Administrator is slow. Save/Restore operation is taking more than the expected time. Please wait while the save/restore operation completes. If the restore operation exceeds 4 minutes on Onboard Administrator, a message appears stating that the save/restore operation could not be completed, however, the operation does complete.

When an Onboard Administrator is discovered, the enclosure that it resides in is created. If this enclosure is daisy chained to other c-class enclosures, then these enclosures are also created. By default, daisy chained enclosures are displayed as c7000 enclosure models. As a result, when c7000 and c3000 enclosures are daisy chained, and the Onboard Administrator is discovered, the c3000 Tower Model enclosure is displayed as a c7000 enclosure. To ensure that the daisy chained enclosures are displayed accurately, you must discover the Onboard Administrator on each of these enclosures.

To correctly identify the xw25p Blade Workstation, you must install Insight Management Agent 7.4.

To associate the Cisco Gigabit Ethernet Switch Module with the HP BladeSystem enclosure it is inserted in, you must update the HP Insight Management Agents to 7.3 or later on at least one blade in the enclosure.

If you have licensed a system for HP Insight Control power management and receive the following error message while attempting to view the **last data collection status** on the **System Page** for the system, Unable to communicate with Management Processor <mpname> in server <servername> because the Management Processor does not have a serial number and(or) network address. Please re-identify the Management Processor and try again., then there might be a problem with duplicate iLOs associated with the system. Use the **All Management Processors** view and identify the iLOs associated with the server. There is one iLO with its name being the IP address of the iLO and another iLO with the serial number of the iLO as its system name. Deleting the iLO with no IP address recorded resolves the issue.

After discovering new servers and their iLO 2 management processors using **Reports→Insight Power Manager**, the task wizard indicates the server is not compatible with Insight Power Manager.

Solution: Insight Power Manager requires an association to exist between the iLO management processor and the server before compatibility can be determined. If you attempt to use the Insight Power Manager tool before this has been determined, you encounter this issue.

- Select the iLO 2 from the system list and execute **Options→Identify Systems** to re-execute the Insight Power Manager compatibility check.
 - or
 - Wait for 15 minutes for Insight Power Manager's periodic system management to re-determine compatibility. After compatibility has been verified, this problem should not reoccur.
-

After applying an iLO Select or Advanced license to the iLO 2 using its user interface, **Refresh Data** is clicked in Insight Power Manager to collect new power history data and a message appears indicating the iLO 2 has no license.

Solution: HP SIM must re-identify the iLO 2 to detect the presence of the new license. Select **Options→Identify Systems** to re-identify the iLO 2 or wait for HP SIM's periodic identification cycle to complete. You can check the status of HP SIM's awareness of iLO 2 license assignment selecting **Deploy→License Manager**.

Insight Control virtual machine management

virt fails to update the change in VM name when performed from Virtual Connect. It is observed that when a VM name is updated from vCenter that is registered on the hosts, the updated name does not reflect on the 'All Systems Page'. However, the change is updated in the host system page after few minutes.

For the VM name to be updated and reflected in the All Systems system list page, initiate an identification task on the host **System Page**.

After you have selected the **Install Linux PSP or ESX agents** and Register VM host options in a Configure or Repair Agents task for ESX 3.5 U4 or later, the VM-host registration task fails because the system shows as Not Responding in Vcenter. Vcenter takes about five minutes for a system to reach a Normal status and therefore fails when HP SIM tries to register the VM host. Re-run the VM-host registration task at a later time when the server is in a Normal state in Vcenter.

HP Smart Update Manager

Online deployment through HP SUM is not supported for Itanium based systems.

To install HP SUM, you must select the following additional libraries on the system running HP SUM:

- Compatibility libraries
- Under Hardware Monitoring Utilities, the following must be selected:
 - lm_sensor-3.1.1-10.el6
 - Under **Systems Management**:
Select **SNMP Support**.
 - Under **Desktops**.
 - Select **X Windows System**.
 - Select **Legacy X Windows System Compatibility**.
 - Select either the **Gnome** or **KDE Desktop**.
 - Under **Development Tools**, the following must be selected:
 - **expect-5.44.1.15-2.el6**.

The prerequisites for Red Hat Enterprise Linux 6 servers - RHEL6 Console Mode:

NOTE: No X console in either x86 or x86_64 - User installs base server with defaults and the following RPMs to run HP SUM in silent mode.

NOTE: The versions below are needed as a minimum. Later versions of these can most likely be used as well.

- lm-sensors-libs-3.1.1-10.el6.<arch>.rpm
 - net-snmp-libs-5.5-27.el6.<arch>.rpm
 - net-snmp-5.5-27.el6.<arch>.rpm
 - kernel-headers-2.6.32-71.el6.<arch>.rpm
 - redhat-rpm-config-9.0-3-25.el6.noarch.rpm
 - kernel-devel-2.6.32-71.el6.<arch>.rpm
 - rpm-build-4.8.0-12.el6.<arch>.rpm
 - gcc-4.4.4-13.el6.<arch>.rpm
-

For Red Hat Enterprise Linux 6 servers - RHEL6 Graphical Mode:

NOTE: This applies to both x86 and x86_64 if the user elects to install the XWindows support.

NOTE: These must be the 32-bit version even under x86_64 architecture as HP SUM and several of the RPMs require 32-bit libraries installed.

NOTE: The versions below are needed as a minimum. Later versions of these can most likely be used as well.

- libuuid-2.17.2-6.el6.i686.rpm
- freetype-2.3.11-5.el6.i686.rpm
- libSM-1.1.0-7.1.el6.i686.rpm
- libICE-1.0.6-1.el6.i686.rpm
- libXi-1.3-3.el6.i686.rpm
- libX11-1.3-2.el6.i686.rpm
- libXext-1.1-3.el6.i686.rpm
- libXcb-1.5-1.el6.i686.rpm
- libXau-1.0.5-1.el6.i686.rpm
- libXrender-0.9.5-1.el6.i686.rpm
- libXrandr-1.3.0-4.el6.i686.rpm
- libXfixes-4.0.4-1.el6.i686.rpm
- libXcursor-1.1.10-2.el6.i686.rpm
- fontconfig-2.8.0-3.el6.i686.rpm
- expat-2.0.1-9.1.el6.i686.rpm
- expect-5.44.1.15-2.el6.<arch>.rpm
- zlib-1.2.3-25.el6.i686.rpm
- libstdc++-4.4.4-13.el6.i686.rpm
- net-snmp-5.5-27.el6.<arch>.rpm

In addition, the build directory for RPMs built from source has changed depending on the name of the user building them. Up through RHEL5, the directory had been `/usr/src/redhat/RPMS/<architecture>`. Under RHEL6, the directory is `/root/rpmbuild/RPMS/<architecture>` if the user is logged in as root and `/$USER/home/rpmbuild/RPMS/<architecture>` for users other than root.

If you are receiving an HP Smart Update Manager Connection Error or Discovery Failed message in the StdOut Task Results for Initial ProLiant Support Pack Install, SSH Install, or Configure or Repair Agents, follow the following troubleshooting tips:

- Ensure your workstation does not have an existing connection to the admin/administrator share on the target IP address. If it does, it prevents HP Smart Update Manager from connecting to the remote server's share because Windows only allows one connection from a client to a server's share. This can be checked by entering `net use` at a command prompt. If there is an existing share to the target IP address, `\admin` share, delete it and try the installation again.
- Ensure that the target IP address server's admin share is accessible. Validate the target server can be accessed by entering `net use x: \\<ip_address_or_dns_name>\admin` for the target server's IP address or DNS name. When the connection is validated, ensure that it is deleted by entering `net use x: /d` at command prompt.
- Ensure the user ID being used to connect to the target IP address server is part of the administrator's group. If it is not, HP Smart Update Manager blocks installation to the target.

- Ensure WMI is enabled and running on all Windows target servers.
- For Linux, ensure the SSH port is not blocked.
- In some rare cases, external storage enclosures can cause HP Smart Update Manager to report a discovery failure. To resolve this problem, disconnect the external storage until the firmware updates are completed.
- For Linux, ensure that the target server can be contacted through SSH and that the `scp` command is available to securely send files to the target server.
- Ensure the firewall ports on any routers in the network as documented in the **Enabling** ports in the HP Smart Update Manager documentation.
- The Symantec End Point Protection product (SEP) blocks HP Smart Update Manager ability to communicate with remote targets if the Network Threat Analysis feature is enabled. Disable this feature while HP Smart Update Manager is in use on the workstation.

HP Service Pack for ProLiant

When the HP Service Pack for ProLiant is uploaded using the **Upload Support Pack** option, HP VCRM as invalid. This occurs because HP VCRM Upload Control fails to process the component with a size of more than 100 MB.

As a workaround, for VCRM to display the HP Service Pack for ProLiant correctly, perform either of the following:

Procedure 51 Displaying HP Service Pack for ProLiant correctly through HP VCRM

1. Click on the invalid SPP link on the VCRM homepage and make a note of the missing component filenames that are marked in red.
2. Extract the missing component manually from the SPP and copy it to the repository.

OR

Place the "Service Pack for ProLiant" ISO file directly into the repository folder.

HP Systems Insight Manager

When HP SIM 7.2 is installed on a Windows 2012 system, the **About** page in HP SIM shows incorrect operating system version as Windows NT(unknown). This is an issue with the JRE currently integrated with HP SIM, where Java is unable to obtain Windows 2012 operating system value. To resolve this issue, download and install JRE version 1.6.0_38-b05.

Text in UI is not translated into other languages and appears in English. This happens when the text is obtained from a system.

Page in HP SIM appears with no content due to a truncated JSP deployment.

Solution: The cause of the error is lack of disk space. HP recommends you delete the `.class` and `.java` files related to the JSP causing the issue (`{HPSIM}\jboss\server\hpsim\work\jboss.web\localhost\`). Deleting the entire `localhost` directory will impact performance because a restart would be required for all JSP pages to be recompiled by JBOSS.

When shutting down HP-UX, sometimes a message indicating HP SIM is being stopped will be missing from the `rc.log`.

Identification

The new SSH identification method cannot be used to form associations between DL100 series systems; such as the DL160 G5 and DL180 G5 and their management processors. There is an incompatibility between the system UUID presented by the system and the UUID presented by the BMC (management processor) firmware.

To get basic hardware data, such as model, serial number, and UUID, from non-HP x86 servers running VMware ESX Server or Linux, you must configure the root user as the Sign-in credential in HP SIM. This is because the Privilege Elevation feature is not used for identification of servers and running `dmidecode` requires the root privilege. In addition, to identify the VMware ESX server as the VMware ESX Host subtype, the WBEM cimserver on the ESX host must be up and working correctly. There are many ways to set these credentials:

- Global sign-in credentials (**Options→Security→Credentials→Global Credentials**)
- System Sign-in credentials (**Options→Security→Credentials→System Credentials**)
- Discovery task Sign-in credentials (**Options→Discovery→Edit→Credentials**)

For ProLiant iLO2's to be properly identified with WS-MAN functionality, the iLO2 credentials must be the first credentials specified in either the discovery credential list or the global credential list when discovery is run. Otherwise, system credentials can be set directly for the system after it is discovered.

Unable to identify ESX 3.x classic servers to have the appropriate system types and subtypes, or no virtual machines can be discovered from the ESX 3.x hosts.

Symptoms:

- The host is not identified correctly in HP SIM with the type Server and subtype as VMware ESX Host, Virtual Machine Host
- The host is discovered correctly in HP SIM with the appropriate types and subtypes. However, no guests are discovered. The Vman page shows the host, but no guests. The virt property page is the one place on the CMS that does show the guests.
- On the ESX host, when attempting to start the WBEM server, the following error is given:

```
# service pegasus start
Processing /var/pegasus/vmware/install_queue/1 [FAILED]

ERROR: See log - /var/pegasus/vmware/install_queue/1.log
```

- When running HP SIM discovery, the following information appears:

```
Running WBEM rules based identification.
Cannot get ComputerSystem WBEM/WMI data from the system

[WBEM] System identified as WBEM instrumented but no usable
WBEM credentials available. Check configuration and rerun
Identification. Root Cause: Identification failed to generate
relevant WBEM credentials for target system.
Corrective Action: Check network and configuration of target
system. Check the following pages to ensure appropriate WBEM
credentials and port number data are provided: Global Protocol
Settings, System Protocol Settings. Rerun Identification and
Data Collection..
```

Solution: Go to <http://communities.vmware.com/message/914939#914939>. Note that the fix above references `/var/pegasus/vmware/install_queue/1` in the install queue. However, the number might vary by installation.

I am unable to identify Windows XP targets through WBEM if Simple File Sharing is enabled.

Solution: Uncheck **Simple File Sharing** by navigating to **Tools→Folder Options→View** or set the security policy **Network access: Sharing and security model for local accounts** to **Classic: Local users authenticate as themselves**.

Installation

To install HP SIM, Framework 3.5 SP1 must be installed on all supported Windows systems. When installing HP SIM 7.2 on a Windows 2012 system, the correct version of Framework is installed. However, you cannot install Framework through the **Add Roles and Features** option available on the server manager.

To workaround this issue, complete the following:

1. Place the operating system image in the CD/DVD drive.
2. From the command prompt, run `xcopy e:\sources\sxs\*.x c:\dotnet35 /s`, specifying the path where the .net package is to be placed.
3. Go to **Server Manager** and click **Add Roles and Features**. The **Feature Selection** page appears.
4. Select **.Net Framework 3.5 Features**, and click **Next**. The **Confirm Installation** page appears.
5. Click **Specify an alternate source path**. Specify the path where Dotnet Framework is placed (same path as in Step 2).
6. Click **Install** and observe that Dotnet Framework is installed successfully.

HP-UX install/execution of partner plug-ins (for example, HP Insight Dynamics - VSE for Integrity) might fail due to failed communication with HP SIM. Reviewing the install logs, daemon service logs and command line command output of partner commands may show long execution time with failed results describing a failure to connect to HP SIM or the message

`java.net.NoRouteToHostException: No route to host (errno:242). Local partner communication to HP SIM occurs using the 'localhost' hostname. This should be set to the loopback IP address (usually 127.0.0.1). This is normally defined in the /etc/hosts file on the CMS.`

However, by default HP-UX systems will resolve hostnames through DNS before looking at this file. If `nslookup localhost` does NOT resolve to the loopback IP address, then you must change the lookup configuration. HP-UX or Linux systems use `/etc/nsswitch.conf` to resolve hostnames, and having `dns` resolve before `files` (`/etc/hosts`) will give the wrong IP Address for localhost. The default for HP-UX is set as:

```
hosts: dns [NOTFOUND=return] nis [NOTFOUND=return] files
```

To resolve this issue, change the configuration to:

```
hosts: files dns [NOTFOUND=return] nis NOTFOUND=return] files
```

Also, be sure the `/etc/hosts` file contains the loopback entry: `127.0.0.1 localhost loopback`.

When HP SIM 6.1 is installed on HP-UX, you should consider monitoring the pgsql logs under `/var/opt/hpsmdb/pgsql` and clear them if they become too large.

HP SIM requires the **DBA Role** privilege for the user during HP SIM installation or upgrade only. However you can select to revoke the **DBA Role** privilege from the user after installation or upgrade is complete.

1. HP SIM installation
 - Create a database user with **DBA Role** privilege on the Oracle database server.
 - Install HP SIM with the database user created for the database.
2. Post installation

After successful installation, stop the HP SIM service.
3. Configure the database user.
 - a. Remove the **DBA Role** privilege from the database user.
 - b. Grant **Unlimited Tablespace** for the database user.

- c. Grant the following **Object Privilege** to all tables and views:
 - INSERT
 - UPDATE
 - DELETE
 - SELECT
 - d. Grant **CREATE SESSION** privilege for database user.
 - e. Grant **truncate** privilege for:
 - associated_device_data
 - consolidatedNodeAuths
4. Restart the HP SIM service.

License Manager

Collection of Lights-out 100 licenses from Lights-out 100 targets are supported beginning with in HP SIM 6.1 and deployment on LO100 targets on G6 servers with latest firmware versions.

When a subscription license for a particular product has expired, license manager's opening table will still show that product has no system limit. The true disposition of licenses for the corresponding product can be determined by opening **Manage Licenses**. If an expected subscription license is not listed, it has expired and is no longer available.

Locale

Certain parts of CLI output might contain system-generated text that always appears in the language indicated by the default CMS locale, not the locale of the user's CLI terminal. This condition can occur following two problems:

- This text might provide a localized property key of the TDef file, which is not allowed for TDef input.
- This text might be identified by one or more question mark (?) character strings appearing in the CLI output.

Solution: The CMS locale is determined by the `globalsettings.props` file. To change the CMS locale and possibly allow the CLI to generate proper locale text, edit the `globalsettings.props` file by running the following command:

To set CMS Locale to Japanese:

```
mxglobalsettings -s -f CMSLocale=ja_JP
```

To set CMS Locale to English:

```
mxglobalsettings -s -f CMSLocale=en_US
```

After you run this command, restart HP SIM.

Managed Environment

When you set the Ignite server on the **Managed Environment** page and then access the page again, you cannot change and save the address again.

Solution: To bypass this problem, modify the Ignite tools from the CLI using the tools' original tdefs, as follows:

Procedure 52 Issue with changing and saving the address of an Ignite server

1. From the CLI, go to the `Tools` directory under the HP SIM install directory on Windows and under `/var/opt/mx/tools` on Linux and HP-UX.

2. Run `mxtool -mf <tool XML> -x force'` where `<tool XML>` for each TDef is as follows:
`iux_tools.xml`
`swm-msa-tools.xml`
`swm-ssa-tools-up.xml`
`swm-ssa-tools.xml`
`hpux\iux_tools.xml`
`hpux\swm-msa-tools.xml`

HP MIBs

The LinkUp and LinkDown traps in `IF-MIB.mib` are redundant traps; these are also present in `rfc1215.mib`. As per the current framework, the redundant traps are not allowed in HP SIM **Traps with same name**.

Change the loading of MIBs. The `IF-MIB.mib` is loaded first and then the `RFC1215.mib`. The `IF-MIB.mib` will be listed in `mibcore.list` and `RFC1215` in `preload.list`. By doing this the LinkUp and linkDown traps from `IF-MIB.mib` will only be registered with HP SIM. The `RFC1215` file will only show four traps **Cold Start, Warm Start, Authentication Failure, egp...**

Do not rename, move, or delete MIB files from the MIBs directory after they are registered.

Solution: For a MIB file to be listed as registered, the MIB file must reside in the MIBs directory.

Onboard Administrator

When an Onboard Administrator system is deleted, health status of the bare metal server systems remain stale. ProLiant OA must be rediscovered to obtain updated health status of the bare metal server systems.

OpenSSH

OpenSSH installation fails on a Windows XP SP3 system.

Solution: Verify that the **Network access: Sharing and security model for local accounts** under **Local Policies**→**Security Options** is set to **Classic - local users are authenticate as themselves**.

Performance

When running HP SIM in an environment that contains a large number of ProLiant systems running the WMI-based Insight Agents, the completed job output in **Tasks & Logs**→**View Task Results** might exceed several thousand files.

Solution: This can result in HP SIM consuming large amounts of memory, task page interface slowdown, or out of memory errors.

If this behavior is noted, the following workaround can be implemented to alleviate the consumption of memory and disk space. The workaround adjusts the retention values for completed tasks and can be altered as desired to reduce resource consumption.

NOTE: This fix only applies to HP SIM instances which are managing a large number of servers (maximum 5000) using WMI.

Add the following script to the `MX.PROPERTIES` file located in the Microsoft Windows directory `\Program Files\HP\System Insight Manager\config` or in the Linux and HP-UX directory `/etc/opt/mx/config`:

MX_JOB_MAX_COMPLETED_JOBS_PER_TASK=3

Recommended value is 3 for greater than 1500 systems

MX_JOB_MAX_COMPLETED_JOB_AGE=7

Recommended value is 7 for greater than 1500 systems

MX_JOB_KEEP_RUN_NOW_HOURS=8

Recommended value is 8 for greater than 1500 systems

After the MX.PROPERTIES file has been modified, restart the HP SIM service to initiate the changes.

Ping

HP recommends you do not disable ping in hardware status polling tasks. If the ping protocol from hardware status polling task is disabled, then other polling protocol statuses like SNMP, WBEM, OOB, WSMAN, and so on will be affected. There will be no polling done for these protocols and the status shown in the UI for these protocols will be that of the previously collected data before disabling ping protocol.

Ports used by HP SIM.

By default, HP SIM uses port 5989 to communicate with the WBEM server of the systems it monitors. To use a different port for this purpose, complete the following:

1. The `wbemporthlist.xml` file used by HP SIM must be altered to add the additional or alternate WBEM port to be used. The file is located in `C:\Program Files\HP\System Insight Manager\Config\Identification`. This example shows where the new lines (in red) must be added to the `<wbemporthlist>` tag in the xml file:

```
<?xml version='1.0' encoding='UTF-8'>
<wbemporthlist>
  <port id='5989' protocol='https'>
    <cimnamespacelist>
      <cimnamespace name='root/cimv2' />
      <cimnamespace name='vmware/esxv2' />
      <cimnamespace name='root/hpq' />
    </cimnamespacelist>
    <interopnamespacelist>
      <interopnamespace name='interop' />
      <interopnamespace name='root/pg_interop' />
      <interopnamespace name='root' />
      <interopnamespace name='root/emulex' />
      <interopnamespace name='root/qlogic' />
      <interopnamespace name='root/ibm' />
      <interopnamespace name='root/emc' />
      <interopnamespace name='root/smis/current' />
      <interopnamespace name='root/hitachi/dm51' />
      <interopnamespace name='root/interop' />
      <interopnamespace name='root/switch' />
      <interopnamespace name='root/cimv2' />
    </interopnamespacelist>
  </port>
  <port id='2718' protocol='https'>
    <cimnamespacelist>
      <cimnamespace name='root/cimv2' />
    </cimnamespacelist>
  </port>
</wbemporthlist>
```

2. Restart the HP SIM service.
3. Right-click the Systems Insight Manager service in Windows Services API, and click **restart** from the dropdown menu.

Privilege elevation

When "DISPLAY_LAST_LOGIN" = 1 in HP-UX, even non-interactive logins, such as used by sudo, emit the **Last login** string. This extraneous data in stderr/stdout can affect tools.

This value can be changed using HP SMH in the **Auditing and Security Attributes Configuration** section of the HP SMH home page. This can be done for the user whose rights have been elevated (typically "root") or set as the system-wide default for all users.

To make these changes, run the following commands:

For an individual user:

```
/usr/sbin/userdbset -u <user> DISPLAY_LAST_LOGIN=0
```

For the system-wide default:

```
/usr/sbin/ch_rc -a -p DISPLAY_LAST_LOGIN="0" /etc/default/security
```

Property pages

I am receiving an error when clicking the **Fans** link on the Property pages **Configuration** tab.

Solution: Upgrade to HP ProLiant WBEM Providers 2.3.

The **Property** pages for the VMWare ESX (Non-Embedded) operating system are not available due to limitations in the WBEM agents.

Reporting

It has been observed that when HP SIM is upgraded from 6.2 to any later version, Enhanced Reports cease to work. If you encounter this issue, you must perform the following steps to solve the problem.

Procedure 53 Correcting issue with Enhanced Reports not working after an upgrade from HP SIM 6.2

1. On Linux or HP-UX:

Navigate to <SIM Installation Directory>\jboss\server\hpsim\work\jboss.web\localhost_org\apache\jsp\mxportal\NewReport

On Windows:

Navigate to: \opt\mx\jboss\server\hpsim\work\jboss.web\localhost_org\apache\jsp\mxportal\NewReport

2. Delete all files in these folders.
3. Go to your browser and refresh the **Enhanced Reports** page and run any report.

NOTE: This does not require the HP SIM service to restart. The changes are automatically detected by HP SIM and Enhanced Reports will work correctly.

In advanced reporting, graph labels may not be displayed properly in the report output.

This can be caused by not having the right Asian fonts installed on the CMS and client system. Ensure that Asian fonts for the desired locale are installed on both the CMS and client system where the browser is installed. In addition the font can be configured to an alternate font in the <HP SIM InstallDir>/config/globalsettings.props file or by running the CLI command: `mxglobalsettings --a EnhancedReportsLogicalFonts=<font name>` where font name can be Dialog or SansSerif. The default value is Dialog.

Security

If HP SIM is installed after HP SMH is installed, the HP SMH 2,048-bit key pair is replaced with the HP SIM 1,024-bit key pair.

Sign-in

User is not able to sign-in to HP SIM when HP SIM is installed on RHEL6.1 64-bit operating system. For HP SIM to work on RHEL6.1 64-bit operating system, the 32-bit library (32-bit(i686) version of PAM-level Red Hat Packager Manager (RPM)) must be installed as part of the operating system installation. This is a prerequisite for HP SIM installation.

SNMP settings

Configuring SNMP settings through Configure or Repair Agents displays corrupt message in task results.

The reported problem will occur if the target system is configured with any localized language except in English. The `/etc/init.d/snmpd` script does not follow localization standards and the error is provided as part of Linux operating system SNMP service.

SNMP traps

After applying Hotfixes or an upgrade, if there is an issue receiving SNMP traps, complete the following:

1. Stop the HP SIM service.
2. Restart Windows SNMP service.
3. Start the HP SIM service.

SSH communication

Domain support for SSH communication:

- **Hyper-V systems**

SSH communication between a CMS and a managed system works properly only when the managed system is in a workgroup. If the managed system is in a domain, then the communication between the managed system and the CMS fails over SSH.

- **Windows systems**

SSH communication between a CMS and a managed system fails if both are in a domain.

Software/Firmware

The **Software and Firmware revision** section under system page of an MSA displays details of both the controllers.

System Page

When WBEM protocol is enabled, incorrect drive information is displayed in the **Logical Volume** section in the **Performance** tab for a blade server.

Solution: To view the accurate drive information, disable the WBEM protocol and enable SNMP protocol. To do so, select **Options**→**Protocol Settings**→**Global Protocol Settings**.

System status

HP SIM shows system with health status OK, although the power status is Major. When Power supplies are grouped, the overall status of the Power Supply group is determined by the Power Supply Redundancy group. This is expected behavior.

Target selection wizard

Cannot launch target selection wizard in Firefox (3.x and above) if HP SIM is upgraded to 7.0 or later.

When you upgrade to HP SIM 7.0 or later and the same Firefox browser is being used for launching older versions of HP SIM, then the target selection wizard will cease to work. Target selection steps appear to be blank, with no control, or the controls might be present, but do not work correctly.

When HP SIM is upgraded, you must clear the Firefox browser cache to avoid issues with the target selection wizard. Perform the following procedure to clear the cache:

1. In the Firefox browser, select **Tools**→**Options**. The **Options** window appears.
2. Select **Advanced**, and then select the **Network** tab.
3. Under **Offline Storage**, click **Clear Now**.
4. Click **OK** to close the **Options** window.

Tasks

The Initial ProLiant Support Pack Install task does not work on Windows 2000 target systems. Likewise, the install portion of the Configure or Repair Agents tool does not work on Windows 2000 systems.

Solution: If the HP Version Control Agent is present on these target systems, then the Install Software and Firmware tool can be used to distribute agents, Support Packs and other components to Windows 2000 systems.

Tools

The message `/tmp/Acmd42947.bat[26]: /usr/dt/bin/dtterm: not found` might appear when running the following tools on HP-UX 11.31:

- Retrieve Bastille Configuration file
- Deploy Bastille Configuration
- Consolidated Logging Wizard
- Configuration Synchronization Wizard

To eliminate this problem:

1. Remove the above tools using the CLI command `mxtool -r -t <tool name>`.
2. Edit the tool definition XML files, replacing instances of `dtterm` and `hpterm` with `xterm`. The above-mentioned tools can be found in the following TDef files:
`security_patch_check.xml`
`clog_windows.xml`
3. Add the tools again using `mxtool -a -f <TDef file name>`
4. Run the tool.

If a user is created with the operator template, then the user is automatically given authorizations to run any CMS tool created with the **Run as** option set to root/Administrator.

Solution: To avoid granting users access to CMS tools, when creating new users, the operator template must not be used and authorization must be configured separately. Note that only HP SIM administrators can create CMS tools.

Ubuntu

Ubuntu Server provides native support for thousands of next-generation applications. This is available in HP SIM through managed system support.

- **On ProLiant servers running Ubuntu with installed agents/AMS**
Discovery and health status monitoring of physical proliant servers will work only if the agents and AMS (in case of Gen8) work satisfactorily.
- **On VM guests running Ubuntu**
Discovery and health of VMs running Ubuntu will work only if these are discovered via the host. Direct discovery using the IP will not work since HP SIM's current design does not support SSH's super user concept.

Upgrade

After upgrade from 7.1 to 7.2 with any intermediate patches, sometimes, you cannot run Enhanced Reports due to irresponsive buttons.

Workaround:

1. Delete all contents under `System Insight Manager\jboss\server\hpsim\work\jboss.web\localhost\_org\apache\jsp\mxportal\NewReport`.
2. Run Enhanced Reports.

When upgrading an HP SIM 6.3 Simplified Chinese system to an HP SIM 7.0 Simplified Chinese system running W2k8-x64 R2, some of the dialog boxes might be garbled. To resolve this issue, update the browser languages preference to Simplified Chinese.

If you are upgrading to HP SIM 5.3 or later on Windows 2008 64-bit, first verify that OpenSSH 3.7.1 is not stuck in a *starting* state. If it is, select **End Process** for the **cygrunsrv.exe** process and any **sshd.exe** processes using the Windows Task Manager.

If HP SIM is installed on a Windows XP system with MSDE as the database, you must manually upgrade MSDE to SQL Server 2005 to upgrade the Windows XP system to Windows Vista.

If you upgrade to Windows Vista on a HP SIM server running Windows XP, you might no longer be able to browse into HP SIM. HP recommends turning off the Windows Vista User Account Control features, and you might/ need to change the privileges of the `SIMinstall\config` directory to get HP SIM running again.

UUID

All server hardware has what is called a UUID available to the operating system through the ROM BIOS. This UUID is use to uniquely identify the hardware regardless of the operating system running on it. While there is a standard way to decode and format/display this value, not all operating system vendors have complied with that standard. For software that did not follow the standard, HP SIM converts this value and displays it in the standard way. This can result in some differences if the UUID is viewed through a given operating system tool such as `dmidecode`.

The SMBIOS stores the 16 bytes of System UUID as:

00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

Dmidecode displays:

00010203-0405-0607-0809-101112131415

UniquelIdentifier in SIM

03020100-0504-0706-0809-101112131415

Virtual Connect Enterprise Manager

Unable to browse to VCEM menu when logged in as read only user. To resolve this issue, install VCEM and other dependent components from Integrated installer component>selection screen. To make the menu visible in HP SIM, configure following settings in browser: **Tools→Internet Options→Security→Custom level**, and then under **Miscellaneous**, select **Allow Script initiated windows without size or position constraints**.

Same settings are applied when the browser security has been set to medium-low.

Virtual identifiers

A new feature of virtual connect is to enable server profiles to have virtual identifiers, such as serial numbers and unique identifiers. These identifiers then move with the profile across server hardware. There are a number of management tools that currently rely on these identifiers to remain stable

for any given hardware platform, if not some serious issues, such as loss of software licenses will occur.

When setting up an environment for virtual identifier support the following steps must be taken for proper operations of the management tools.

1. Upgrade HP SIM to version 5.2 Update 2 or later.
2. For any server that will have a profile with a virtual identifier, upgrade the ROM BIOS to the latest version to ensure it contains virtual identifier support.
Note The server hardware must be listed in the virtual ID support matrix.
3. Upgrade the agents and WMI providers on the servers that will be used for virtual identifiers. (See the version table below for proper versions).
4. Upgrade the firmware for the Onboard Administrator to version 2.25 or later.
5. On the virtual connect Ethernet module, upgrade the virtual connect firmware to version 1.3 or later. Do not enable virtual identifiers at this time.
6. On the virtual connect Ethernet module, enable virtual identifiers.
7. You may now create and assign profiles with virtual identifiers.



WARNING! If you do not follow the specific instructions for enabling Virtual Identifiers in your environment and you enable the feature without the proper agent revisions, iLO firmware, infrastructure orchestration firmware, System ROM revisions, and HP SIM version, then systems might appear multiple times and systems might not properly be associated with systems. If that happens, upgrade to all of the latest software prescribed in the c-Class chassis. You might also need to delete discovered systems in the chassis and rediscover them.

Supported Software and Firmware

Note: Failure to meet the minimal revision of any of the listed components can result in virtual identifiers not working properly resulting in the loss of licenses in HP SIM, in issues obtaining proper warranty information, or result in orphaned systems showing in the system list.

The table below outlines the minimal versions required by management tools such as HP SIM and Remote Support Pack to properly operate.

Table 18 Minimal versions

Product	Version
Virtual Connect Manager	2.0x, 2.1x, and 2.3x
Onboard Administrator	2.30
Integrated Lights-Out	1.6
Server ROM	(see supported server matrix for Virtual Connect)
ProLiant Support Pack / SNMP agents	8.1
ProLiant Support Pack / WMI providers	2.2
Systems Insight Manager	5.3 or later

Virtual machines

HP Insight Management WBEM Providers and SNMP agents must not be installed on a virtual machine guest operating system. Installing the providers or agents on a guest operating system causes HP SIM to have excessive timeouts when data is requested or WBEM Indication Subscriptions are created.

The installer for HP Insight Management WBEM Providers 2.2.x and earlier does not prevent installation on a guest operating system. The installer for version 2.3 and beyond automatically prevents the installation of the providers on a guest operating system.

If the WBEM providers or SNMP agents have been installed on a guest operating system, uninstall and re-identify the managed system in HP SIM.

VMware

The name of the temperature sensors might be incorrect. This is a known issue in the VMWare provider and will be addressed in a future release of VMWare providers.

WBEM

WBEM is no longer supported on HP servers. The last servers to support WBEM were the G6 servers. Therefore, HP SIM will not identify the operating system details properly for RHEL 5.7 Xen and KVM servers.

WBEM indications

Current P9500 embedded SMI-S does not support WBEM indications. WBEM indication will be supported from V05 firmware version.

For a CVAE 7.2 server to receive WBEM indications from XP arrays in HP SIM 7.1, the below configuration changes need to be performed on CVAE 7.2 server.

Procedure 54 Configuration for a CVAE 7.2 server to receive WBEM indications from XP arrays

1. Create the `.ind.keystore` file by executing:

```
keytool.exe -genkey -keystore .ind.keystore -storepass indssl  
-validity 365 -keyalg RSA -keysize 2,048
```
2. After importing HP SIM certificate in CVAE 7.2, the truststore file is creating as `indtruststore` instead of `.ind.truststore`. You must rename `indtruststore` file to `.ind.truststore`.

HP SIM doesn't support WBEM Indications on ESL G3 tape library with embedded SMI-S(without CVTL)

WMI Mapper

When WMI Mapper is installed on a Windows 2008 R2 CMS, the WMI Mapper service may fail to start with the "NT SERVICE\MAPPER" user and the WMI Mapper Indications service might fail to start with the "NT SERVICE\WbemConsumer" user. This occurs on a Windows 2008 R2 CMS that is part of a domain that's security policy is being controlled by a domain controller, in which the above two users are not given the *log on as service* right.

The WMI Mapper and WMI Mapper Indications services fail to start and while trying to start these services from the **services.msc** console, the following error appears:

Windows could not start the Pegasus WMI Mapper service on Local Computer. Error 1069: The service did not start due to a logon failure.

A more detailed error is also listed in the Systems Logs of the Windows Event Viewer.

The problem occurs because in Windows 2008 R2, Mapper and Mapper Indications Services are started with users having lower privileges. By default a standalone Windows 2008 R2 server will have these users with the said privileges. However in the case of a server whose security policies are controlled by a domain controller, these users might be removed from the default set of users and hence the services will not start.

You can choose to follow any one of the below workarounds based on your requirements:

- You change the Mapper and Mapper Indications Service to start with a privileged user account such as the "localSystem" account. This can be made by editing the properties of each of the service using the "services.msc" console
- You can choose to give the following two users "NT SERVICE\WMI Mapper" and "NT SERVICE\WbemConsumer" the "log on as a service" right using the "User Rights Assignment" option in the Security Policy Editor (secpol.msc).

If you have created subscriptions on a Windows managed system and then elect to change the WMI Mapper proxy or install a WMI Mapper on the managed system, you must first unsubscribe for WBEM events, change the proxy, re-identify the systems, and then resubscribe for WBEM events. If you do not unsubscribe for the WBEM events, HP SIM will no longer receive indications from the managed system.

C HP SIM Dynamic Ports

There are three main processes in HP SIM:

- `mxdomainmgr`
- `mxdtf`
- `mxinventory`

These processes communicate with each other using Secure RMI connections (TCP).

HP SIM does not use any specific port. It uses anonymous ports based on the underlying Java RMI implementation which uses the User ports (for example, 1024 – 49151 on Microsoft Vista, Microsoft 2008 and above operating systems). HP SIM processes use different ports on every restart.

- Though Java RMI is used on various user ports, HP SIM listens only on “localhost” such that these services are not exposed outside the system running HP SIM, for consumption. These ranges can be safely blocked in a firewall configuration for incoming requests from outside hosts.
- The `mxdtf` process listener port can be configured in the configuration file, `mx.properties`, by setting `MX_PORT` to the appropriate value. However, if this value is missing, HP SIM defaults to 2367.
- In addition to inter-process communication, these processes perform their regular activities, for example data collection using SNMP / WBEM / SSH etc. from a managed node. Under these situations, the processes use any of the dynamic ports (both TCP and UDP), for outgoing connections.

HP SIM uses various user ports in the range of 1024 to 65535 (using TCP and or UDP) for inter-process communication among the various HPSIM processes. This range of ports can be safely blocked in a firewall configuration for incoming requests from outside hosts.

- Microsoft Windows 2003
- Microsoft Windows Vista, Microsoft Windows 2008 and above

Windows 2003

Microsoft Windows 2003 Microsoft Windows 2003 uses a default port range of 1025 through 5000 as the dynamic client port range for outgoing connections. To avoid port conflicts, HP SIM installer, as part of the installation process, reserves the following ports, if it detects installation on Microsoft Windows 2003 Operating System. The dynamic ports shown in [Table 19 \(page 200\)](#) refer to outgoing connections for both TCP and UDP.

Table 19 HP SIM Dynamic Ports Range for Microsoft Windows 2003

From Port	To Port	Count
1124	1126	3
1433	1434	2
1758	1759	2
1779	1780	2
2301	2301	1
2367	2367	1
2381	2381	1
4011	4011	1
4095	4096	2
50000	50015	16

Microsoft Windows Vista, Microsoft Windows 2008 and Above

To comply with Internet Assigned Numbers Authority (IANA) recommendations, Microsoft increased the dynamic client port range for outgoing connections in Windows Vista, Windows Server 2008, and all of its later operating systems. The default port range is now 49152 through 65535. On these Operating Systems, to avoid port conflicts, HP SIM installer, as part of the installation process, sets the following ports for dynamic ports. The dynamic ports shown in [Table 20 \(page 201\)](#) refer to outgoing connections for both TCP and UDP.

Table 20 HP SIM Dynamic Ports Range for Microsoft Windows Vista, Microsoft Windows 2008 and above

From Port	To Port	Count
51500	65536	14036

D Protocols used by HP SIM

HP SIM uses many different management protocol standards. This capability enables HP SIM to provide management support for a wide array of manageable systems.

SNMP

Simple Network Management Protocol (SNMP) is one of the standard protocols for managing devices on a network. The popular versions of this protocol include SNMPv1 (the initial implementation), SNMPv2c (which provides additional data types and operations but similar to SNMPv1 in terms of security) and SNMPv3 (which provides security features that were missing in the previous versions).

HP SIM is a management tool which lays the foundation for other management solutions from HP like HP Insight Control, HP Matrix Operating Environment (Matrix OE) and HP CloudSystem Matrix. While HP SIM is available for Windows, Linux and HP UX operating systems and supports SNMPv1 till 7.2.0, it will support all versions of SNMP starting from version 7.2.0.

SNMPv1 (and similarly SNMPv2c) imposes variety of threats not limited to masquerading, spoofing, information modification, disclosure and denial of service. SNMPv3 focuses on security in terms of authentication and authorization. Also from a standards perspective, at a minimum, an SNMPv3 implementation should support user-based Security Model (USM) for authentication and View-Based Access Control Model (VACM) for authorization.

HP SIM enables administrators to configure such that it could work with SNMPv1 only mode, mixed mode or in SNMPv3 only mode. While SNMPv1 only mode will be useful for backward compatibility, SNMPv3 only mode will help security conscious customers to meet compliance such as Federal Information Processing Standards (FIPS). The mixed mode will be helpful in an environment where multiple versions of SNMP exist.

HP SIM provides support for configuring SNMP specific parameters at individual managed node level and at global level and supports the following features:

- Manage Users / Credentials
- Discovery and Identification
- Data Collection
- Periodic collection of component status
- Process traps / notifications

HP SIM supports the following SNMPv3 specific features:

- User-based Security Model (USM)
- MD5, SHA algorithms for authentication protocols
- AES (128, 192, 256), DES and 3DES algorithms for privacy protocols

NOTE: While HP SIM 7.2.0 supports TRAP (all versions of SNMP), INFORM will be supported in future releases.

HP SIM supports all versions of SNMP across all of the supported operating systems - Microsoft Windows, RedHat Enterprise Linux (RHEL) , SuSE Linux Enterprise Server (SLES) and HP UX.

Windows

Microsoft ships and supports its own SNMP trap receiver, typically installed as a Windows Service, "SNMP Trap Service", and listens for SNMP traps on port 162 on Windows. Also, the Microsoft SNMP Trap Service acts as a single trap receiver for multiple SNMP managers installed on the same host and thus allow co-existence with other tools. For example, HP SIM and HP Network Node Manager could be installed on the same Windows box and both can receive traps from the managed host through the common Microsoft SNMP Trap service.

From a standards perspective, Microsoft SNMP supports only SNMPv1 and SNMPv2c. Microsoft doesn't support SNMPv3 and has no plans to support it. Since the default port 162 will be used by the Microsoft SNMP Trap service, HP SIM supports an additional port 50005 which can receive all versions of SNMP trap. Thus on Microsoft Windows platform, HP SIM supports dual SNMP stack, one leveraging Microsoft SNMP Trap service another built-in Java stack.

In order to support Microsoft SNMP Trap service, HP SIM has a trap forwarder component which will register with the Microsoft SNMP Trap service and forward traps to HP SIM. While registering, HP SIM will provide the directory location where traps will be dumped in XML file. These XML files will then be processed by HP SIM and cleared accordingly.

While the built-in Java stack might simplify the support from HP SIM perspective, it doesn't provide co-existence solutions with other SNMP managers. Hence, by default HP SIM configures with Microsoft SNMP Trap service on port 162 and built-in Java stack on port 50005, mainly considering backward compatibility for those customers who are upgrading HP SIM. However, HP SIM allows the Administrator to configure the desired SNMP stack and port.

Procedure 55 Using the built-in Java SNMP stack

1. Stop HP SIM service. For example, use the `mxstop` command.
2. Open the `globalsettings.props` file in a text editor (file is typically located in `C:\Progaam Files\HP\System Insight Manager\config` folder.)
3. Change the value for **`snmp_java_trap_receiver`** to true.
4. Change the value for **`SnmpTrapPortAddress`** (if you need to change the port as well).
5. Save and close the file.
6. Ensure to stop and disable the Microsoft SNMP trap service.
7. Start HP SIM service (For example, use the `mxstart` command.)

Procedure 56 To revert from Java SNMP stack to Microsoft SNMP trap service

1. Stop HP SIM service. For example, use the `mxstop` command.
2. Open the `globalsettings.props` file in a text editor (file is typically located in `C:\Progaam Files\HP\System Insight Manager\config` folder.)
3. Change the value for **`snmp_java_trap_receiver`** to false.
4. Change the value for **`SnmpTrapPortAddress`** (if you need to change the port as well)
5. Save and close the file.
6. Ensure to stop and disable the Microsoft SNMP trap service.
7. Start HP SIM service (For example, use the `mxstart` command.)

NOTE: If Microsoft SNMP Trap service is restarted after HP SIM is started, please ensure to restart HP SIM. Otherwise, HP SIM may not be able to receive SNMP traps.

As mentioned earlier, 50005 port is used in addition to port 162 for receiving all versions of SNMP traps; to change the port from the default 50005, modify the value of **`snmpv3_java_trap_port`** property in `globalsettings.props`. However, please note that the value/port configured for **`SnmpTrapPortAddress`** and **`snmpv3_java_trap_port`** cannot be the same (unless **`snmp_java_trap_receiver`** is set to true and Windows SNMP Trap service is disabled).

HP-UX and Linux

In the case of HP UX and Linux operating systems, HP SIM supports only built-in Java SNMP stack which by default binds to port 162. However, if the port needs to be changed to a different one, follow the procedures mentioned below,

Procedure 57 Assigning HP SIM to use a different port

1. Stop HP SIM service. For example, use the `mxstop` command.
2. Open the `globalsettings.props` file in a text editor (file is typically located in `/etc/opt/mx/config` folder.)
3. Locate and change the value for **`SnmpTrapPortAddress`**.
4. Save and close the file.
5. Start HP SIM service (For example, use the `mxstart` command.)

NOTE: HP SIM does not receive traps from the application using port 162 unless the application is configured to forward traps to the port assigned to HP SIM. If the **SnmptTrapPortAddress** entry is deleted, HP SIM defaults to port 162.

HTTP

HP SIM also takes advantage of the industry standard HTTP protocol (used to transfer information over the World Wide Web) for transportation of management information. Many systems support some kind of configuration "home page" that is supported over HTTP or the secure HTTPS protocol. HP SIM attempts to find HTTPS servers running on systems if the **Global Protocol Settings** page has this enabled.

If you have changed the http or https port number on a managed system, then perform the following steps to enable HP SIM to identify the port correctly. For management processors, data from http/https is used for identification.

Procedure 58 Enabling HP SIM to identify ports correctly

1. Open the `additionalWsDisc.properties` file located under `<SIM_INSTALL_DIR>\config\identification` on Windows systems, and `/etc/opt/mx/config/identification` on Linux and HP-UX systems.
2. Add the following entries for systems other than management processors (management processors include iLO and Onboard Administrator):

```
<PORT_NO>=Secure Web Server Interface, ,true,false, ,https  
<PORT_NO>=Web Server Interface, ,true,false, ,http
```

Where `<PORT_NO>` is the http/https port number that is configured on the managed system.
For example: If the http port number is configured to 83, then following entry is added:
`83=Web Server Interface, ,true,false, ,http`
3. If the managed system is a management processor, like iLO or Onboard Administrator, then add the following entry:

```
<ORT_NO>=Web Server Interface,  
,true,false,com.hp.mx.core.tools.identification.mgmtproc.MgmtProcessorParser,http
```

For example: If the http port number of the iLO is changed to 83, then following entry will be added `83= Web Server Interface,
,true,false,com.hp.mx.core.tools.identification.mgmtproc.MgmtProcessorParser,http`

WBEM

WBEM is one of the newest management protocols. This protocol leverages the industry-standard CIM as defined by the DMTF. HP SIM can communicate to systems directly using the WBEM protocol or to the Windows WMI systems using the WMI Mapper Proxy. HP SIM uses WBEM to communicate with storage system **SMI-S WBEM providers** and HP-UX providers. HP has been leading this effort through its association with the Distributed Management Task Force (DMTF). WBEM is an initiative supported by HP, Microsoft, Intel, BMC, Cisco, and 120 other platform, operating system, and application software suppliers.

When WBEM is enabled, the management console can obtain information from any system that supports WBEM. For WBEM to work, you must provide the correct user name and password for the given system. WBEM enables a larger set of server and storage manageability data to be collected and displayed on the **System Page** and in reports. The presence of WBEM enables the **Properties** pages and enables WBEM indications (events) to be displayed in event collections. Without HTTPS enabled, HP SIM does not discover any WBEM-based features on a system. Support for non-HP systems has been expanded starting with HP SIM 6.0.

NOTE: HP SIM supports WBEM over HTTPS to ensure user supplied WBEM name and password pairs are protected.

NOTE: OpenWBEM is not supported.

Remote Method Invocation (RMI)

Java RMI is used within the CMS only for inter-process communication.

Remote Wake-Up

Remote Wake-Up refers to the ability to remotely turn on a system that is in a soft-off power state. Systems that support the Advanced Configuration and Power Interface (ACPI) should be awakened transparently by any network activity to the system. Alternatively, a system might support the Magic Packet technology. When a system is turned off, the Magic Packet — capable network interface card (NIC) is still powered on and monitoring traffic. The system will be powered on, if it receives the Magic Packet targeting it.

Internet Control Message Protocol (ICMP)

ICMP is used during automatic system discovery and prior to other requests to a system to ensure the system is responding. An ICMP echo request, also known as a ping, is sent to the system's IP address. Receipt of a proper reply indicates the system is up and responding.

NOTE: HP SIM can be configured to use TCP as a ping, instead of ICMP, from the **Global Protocol Settings** page.

Lightweight Directory Access Protocol (LDAP)

LDAP 3 is used during execution of a Directory Group tool to communicate with the configured directory server to collect information about systems configured in the directory.

Simple Object Access Protocol (SOAP)

SOAP is used by partner applications to communicate with HP SIM. It is primarily XML over HTTPS.

Protocol functionality

The following table displays descriptions of management protocols displayed under **Management Protocols** on the **System Page** which displays protocols that have responded when attempting to identify the system.

NOTE: The CMS initiates the requests for all protocols except events.

Management standard	Description	Functionality when enabled
CIM	A common definition of management information for systems, networks, applications, and services.	System identification, inventory, events
CIM-XML	A protocol using XML over HTTP to exchange CIM information; part of the WBEM suite of standards.	System identification
HTTP and HTTPS	HTTP is another primary protocol used to acquire data about managed systems during identification. HTTP is not a secure protocol and can be easily viewed on the network. The secure version of HTTP is called HTTPS and is described later.	System identification, management tool launch, agent configuration
ICMP	ICMP is a required protocol tightly integrated with IP. ICMP messages are delivered in IP packets and are used for out-of-band messages related to network operation. HP SIM can use ICMP messages to ping a managed system. However,	Provides system reachability (ping) check during system discovery and before other operations

Management standard	Description	Functionality when enabled
	some routers block ICMP messages so HP SIM provides an alternative ping using TCP.	
MIB	Part of the SNMP specification, the MIB is a model of the information to be managed through SNMP. It is equivalent to the CIM defined by WBEM.	System identification, inventory and events
SNMP	SNMP is widely used for management but the widely implemented versions 1 and 2 have weak security. While no set operations are used by HP SIM, read access to system data might be visible on the network. SNMP is UDP-based. In many environments it is not considered a suitable protocol to pass through the firewall. Because SNMPv1 has a simple, clear-text community, it provides a low level of security. However, SNMP can be suitable for some environments in which the network used for managing systems is relatively controlled.	System identification, Inventory and events
SSH	SSH is used for remote command execution. HP SIM uses SSH to run commands on managed systems.	Remote tool execution
SMASH	A DMTF initiative for common server management which enables vendor-independent management applications.	Consistent server management across vendors
SMI-S	An SNIA standard for storage management using WBEM.	System identification
WBEM	A DMTF program with widespread industry support with a set of standards including CIM, CIM-XML, and WS-Management. The CIM-XML protocol is most widely used with WBEM today, and the term WBEM is often used to mean this protocol. Note: Configure firewalls to allow the CMS to communicate with managed systems through default port 5989. If you have modified the default port setting for your WBEM provider, you must configure your firewall for the port number your WBEM provider on which it is actually configured.	Identification, inventory, and events
WS-Management	A DMTF standard for exchanging management information using web services. You can use WS-Management to transport CIM as an alternative to CIM-XML.	Identification, inventory, and events
WMI	WMI is Microsoft's implementation of WBEM. WMI runs over Distributed Component Object Model (DCOM) , which in turn, uses RPC. For Windows systems behind a firewall, HP recommends installing the WMI	Identification, inventory, and events

Management standard	Description	Functionality when enabled
	Mapper on a managed system in the secure network. This mapper allows standard CIM-XML requests through the firewall, and they are mapped to WMI requests on the managed system.	

Configuring protocol settings in HP SIM

You can use HP SIM to set protocol settings for all systems, for a group of systems, or for an individual system. You can control the way HP SIM uses these protocols, such as configuring default timeouts and retries, or disabling HP SIM's use of the protocol entirely.

To set protocol settings for all systems, access the **Global Protocol Settings** page in one of the following ways:

- Select **Options**→**Protocol Settings**→**Global Protocol Settings**.
- From the **Discovery** page, click **Configure global protocol settings** in the **Discovery configuration** section.

Setting protocol settings for a single system or group of systems, access the **System Protocol Settings** page in one of the following ways:

- From the **All Systems** page, click the **System Name** link of the system to go to the **System Page** for that system, and then click the **System Protocol Settings** link on the **Tools & Links** tab page.
- From the HP SIM menu, select **Options**→**Protocol Settings**→**System Protocol Settings**, and then select the single system to set its protocol settings.

Procedure 59 Setting protocol settings for a single system

1. Access the **System Protocol Settings** page by selecting **Tools**→**System Information**→**System Page**.
2. Select the target system.
3. Click **Run Now**.
4. Select **Links**→**System Protocol Settings**.

E Data Collection

After HP SIM collects data initially during the identification process, you can schedule a Data Collection task to specify systems and run the task with different schedules. In addition to the default Initial and Bi-Weekly Data Collection tasks built in to HP SIM, you can set new data collection tasks targeting specific [managed systems](#). If you are scheduling to **Overwrite existing data set (for detailed analysis)**, formerly known as Single Instance Data Collection task in Insight Manager 7, having it run once per week (smaller networks) to once per month (larger networks) should be adequate. If you are scheduling to **Append new data set (for historical trend analysis)**, it might be beneficial to run data collection more frequently, perhaps once per hour for your most important systems, realizing it consumes database storage space.

To create a Data Collection task from the toolbar, select **Options→Data Collection**.

NOTE: To enable data collection to collect data from any of the protocols used by HP SIM, the corresponding protocol must be enabled, and the appropriate protocol settings and credentials must be specified, globally or for the specific target system.

NOTE: To enable collection of [WMI](#) data from WMI-instrumented systems, a WMI Mapper Proxy must have been set and specified through **Options→Protocol Settings→WMI Mapper Proxy**.

Append new data set (for historical trend analysis)

The **Append new data set (for historical trend analysis)** option maintains trend information in separate historical entries. You can use the historical perspective for trend and usage analysis because records change over time. Information gathered by data collection is used in Snapshot Comparison and reports and can be used as criteria in system collections. With **Append new data set (for historical trend analysis)**, data detailing the system history is collected. Use **Append new data set (for historical trend analysis)** sparingly to track problem systems or problem usage times. Do not overuse this task because it can create a considerable amount of data to be stored.

 **CAUTION:** Do not delete the standard data collection task without replacing it with a substitute task that achieves a similar result. For example, removing the Data Collection task removes the capability for historical analysis and updating any information shown in reporting tables. You must refresh the page to see new data in reports.

Overwrite existing data set (for detailed analysis)

The **Overwrite existing data set (for detailed analysis)** option overwrites any previous information collected.

You can view the current Data Collection report from the **Tools & Links** tab of the **System Page**, which you can reach by selecting a system in a collection.

Running data collection consumes noticeable network resources. Proper scheduling might be appropriate.

 **IMPORTANT:** Multiple instances of the same Status Polling or Data Collection tasks do not run simultaneously.

Initial data collection

The Initial Data Collection task is used to collect information from many systems that have SNMP or WBEM running (for example, serial numbers and model numbers). This task is set to run by default when a new system or event meets the search criteria. You can view the Data Collection Report for a system after data has been collected by selecting it from the system table view page. This action displays the **System Page**, where you can select the **Data Collection Report** link from the **Tools & Links** tab. Other report formats are available from the Reporting tool.

Bi-weekly data collection

The Bi-Weekly Data Collection task runs the **Overwrite existing data set (for detailed analysis)** option on all systems in the system default collection. The default schedule is to run every two weeks on Saturday at 12:00 a.m. You can view the Data Collection Report for a system after data has been collected by selecting it from the system table view page. This action displays the **System Page**, where you can select the **Tools & Links** tab and then click **Data Collection Report**.

F Default system tasks

Polling tasks track the [health status](#) of systems in associated collections. Hardware status polling must occur periodically to determine when systems go offline or when hardware degrades. You can customize polling tasks for specific systems to run at scheduled times. You can also create polling tasks with different collections to meet your needs.

You can configure polling tasks to take place based on the receipt of an event. Event polling tasks are associated with event collections. For example, you might set up a hardware status polling task for when traps are received from a system.

When a polling task is set up to run as the result of a change in an event collection, the polling task is applied to all systems generating events that match the given collection.

NOTE: HP does not recommend scheduling a polling task based on periodic event collection. The task would run on the set of systems for each event in the associated collection.

NOTE: If you remove a hardware status polling task, systems continue to be discovered, but the status on them is not updated. If you remove the Daily System Identification task, you would no longer detect changes in management on systems.

The following default tasks are available on the **View All Scheduled Tasks** page:

- Use this task to collect data. This task runs on all systems in the **Data Collection List** collection. The default schedule sets the task to run every other Saturday at noon.
- Use this task to gather information about systems such as networking systems. By default, this task runs once a day. The information is identified and stored in the database.
 - Single Sign On and STE support on a managed system
 - Type of management protocol on the system (HTTP, SNMP, and WBEM)
 - Type and subtype of system (server, storage, switch, router, and so on)
 - Product name of the system
 - Operating system name and version
 - Web Agents running on the system
 - Web-based software running on the system (for example, printer management software)
 - System associations with management processors (for example, a system and its Remote Insight board)
 - Storage proxies and related storage systems
 - Wake-on-LAN information
- Includes events that are transient and happen frequently, but do not generally indicate hardware failures. For example, link up, link down, and authentication events. These events fill the event database tables, but do not add value to the hardware event history.
- This task deletes events older than 90 days and can help maintain HP SIM by limiting the total number of events. By default, this task is disabled. To enable the task:
On the **All Scheduled Tasks** page, click **Enable**.
In some installations there might be high volumes of events. If so, consider using this task and event collections as models and creating an event collection for events older than 30 days (for example), and then creating a task to delete events older than 30 days.
- This task collects status information through management protocols (SNMP, WBEM, and so on) for systems that are not Server, Cluster, or Management Processor type. By default, this task polls every 10 minutes and at start-up.

NOTE: If you discover more than 500 systems, HP suggests you change the interval to something greater than 10 minutes (for example, 15 minutes for every 1,000 systems).

- This task collects status information for SNMP, or WBEM systems that are Server, Cluster, or Management Processor types. By default, this task polls every 5 minutes and at start-up.

NOTE: If you discover more than 500 systems, HP suggests you change the interval to something greater than 5 minutes (for example, 10 minutes for every 1,000 systems).

- This task runs when a system goes from a disabled state to an enabled state. You could use this task to get the latest status after a planned maintenance window on a system that was set to disabled. This should reflect the entire category (inventory, software baseline, and so on) in the Data Collection report.
- Hardware status polling should reflect the proper status of the Onboard Administrator and this status must match with the XML reply data.
- This task collects *static* information from a number of systems that have WBEM, or SNMP running (for example, serial numbers and model numbers).
- This task runs hardware status polling on systems that are newly discovered. Therefore, you do not need to wait for the periodic tasks to run before the system has a valid status.
- This task determines software version update status and is set to run every seven days by default at midnight. You can edit this task or manually run it at any time.
- This task runs the software version tool when a system changes from a disabled state to an enabled state so that the status of the software loaded on the system is kept current in HP SIM.
- This task checks event configuration on all systems and is scheduled to run every day. The **Weekly Check Event Configuration** task can be edited.

Biweekly Data Collection

Use this task to collect data. This task runs on all systems in the **Data Collection List** collection. The default schedule sets the task to run every other Saturday at noon.

System Identification

Use this task to gather information about systems such as networking systems. By default, this task runs once a day. The information is identified and stored in the database.

- Single Sign On and STE support on a managed system
- Type of management protocol on the system (HTTP, SNMP, and WBEM)
- Type and subtype of system (server, storage, switch, router, and so on)
- Product name of the system
- Operating system name and version
- Web Agents running on the system
- Web-based software running on the system (for example, printer management software)
- System associations with management processors (for example, a system and its Remote Insight board)
- Storage proxies and related storage systems
- Wake-on-LAN information

Old Noisy Events

Includes events that are transient and happen frequently, but do not generally indicate hardware failures. For example, link up, link down, and authentication events. These events fill the event database tables, but do not add value to the hardware event history.

Events Older Than 90 Days

This task deletes events older than 90 days and can help maintain HP SIM by limiting the total number of events. By default, this task is disabled. To enable the task:

On the **All Scheduled Tasks** page, click **Enable**.

In some installations there might be high volumes of events. If so, consider using this task and event collections as models and creating an event collection for events older than 30 days (for example), and then creating a task to delete events older than 30 days.

Status Polling for Non Servers

This task collects status information through management protocols (SNMP, WBEM, and so on) for systems that are not Server, Cluster, or Management Processor type. By default, this task polls every 10 minutes and at start-up.

NOTE: If you discover more than 500 systems, HP suggests you change the interval to something greater than 10 minutes (for example, 15 minutes for every 1,000 systems).

Status Polling for Servers

This task collects status information for SNMP, or WBEM systems that are Server, Cluster, or Management Processor types. By default, this task polls every 5 minutes and at start-up.

NOTE: If you discover more than 500 systems, HP suggests you change the interval to something greater than 5 minutes (for example, 10 minutes for every 1,000 systems).

Status Polling for Systems No Longer Disabled

This task runs when a system goes from a disabled state to an enabled state. You could use this task to get the latest status after a planned maintenance window on a system that was set to disabled. This should reflect the entire category (inventory, software baseline, and so on) in the Data Collection report.

Hardware Status Polling for Superdome 2 Onboard Administrator

Hardware status polling should reflect the proper status of the Onboard Administrator and this status must match with the XML reply data.

Data Collection

This task collects *static* information from a number of systems that have WBEM, or SNMP running (for example, serial numbers and model numbers).

Hardware Status Polling

This task runs hardware status polling on systems that are newly discovered. Therefore, you do not need to wait for the periodic tasks to run before the system has a valid status.

Version Status Polling

This task determines software version update status and is set to run every seven days by default at midnight. You can edit this task or manually run it at any time.

Version Status Polling for Systems no Longer Disabled

This task runs the software version tool when a system changes from a disabled state to an enabled state so that the status of the software loaded on the system is kept current in HP SIM.

Check Event Configuration

This task checks event configuration on all systems and is scheduled to run every day. The **Weekly Check Event Configuration** task can be edited.

Status polling

Polling tasks track system health status for systems in the system list. They provide a simple means of assessing system health in the event that an SNMP trap or other event was not properly delivered to the management console. Hardware status polling must occur continuously to determine when systems go offline or performance degrades. You can customize polling tasks for specific systems to run at scheduled times. You can also create new polling tasks with different system or event lists to match your specific requirements.

The following default polling tasks exist:

- **Software Status Polling.**

Used to determine software version update status. This task is set to run every seven days, on Wednesday at midnight, by default. You can edit the task and run it at any time. This task performs the following functions:

- Retrieves software and firmware inventory from systems.
- Determines the software and firmware update status.
- Sorts versions in the database.

To access Software Status Polling, select **Options→Status Polling→Software Status Polling**.

- **Hardware Status Polling.**

Used to track system status:

- **Hardware Status Polling for Non servers.** Used to collect status information for target systems that are not of a server, cluster, or management processor type. This task is configured to poll every 10 minutes and at startup by default. It does not send status change events.
- **Hardware Status Polling for Servers .** Used to collect status information for SNMP systems of type server, cluster, or management processor. This task is configured to poll every 5 minutes and at startup by default. It sends status change events that can be used set up a notification task based on the event.

To access Hardware Status Polling, select **Options→Status Polling→Hardware Status Polling**.

G Host file extensions

Hosts files are used during discovery to manually add multiple systems to the HP SIM database. Hosts files typically contain IP addresses, system names, system name aliases, and user comments. The hosts file that you create can contain additional information about systems. The information appears as one or more comments that precede the hosts file entry for the system. Unless other values are specified, the default values are used.

Table 21 Hosts file system information

Parameter	Keyword
system type	TYPE
SNMP timeouts	SNMP_TIM
SNMP retries	SNMP_RET
SNMP read community	SNMP_MON
SNMP write community	SNMP_CON

You can modify the hosts file to substitute a value for the defaults for one entry or change the default for all subsequent entries. To change values for a single-system entry in a hosts file, add a statement to the hosts file as a comment on the line before the host entry, as shown in the following example. The statement applies only to the system it precedes. In the following example, the default TYPE is changed to "server" for the system EngProliant.

Table 22 Changing default hosts file parameters

Keyword statement	Hosts file entries
#\$IMXE:< Keyword=value >	#\$IMXE: TYPE=server
For example: #\$IMXE: TYPE=server	16.26.176.92 EngProliant.compaq.com EngProliant #user comments

To change the default globally so that it affects the next file entry and all subsequent entries, use a statement similar to the following example. The default is changed to "router" for the next entry. Router remains the default for all entries until another #\$IMXE_DEFAULT statement changes that value. If a single instance of TYPE is changed by a #\$IMXE statement, the default is not used only for the next entry and then reverts to back "router".

Table 23 Globally changing hosts file parameters

Keyword statement	Hosts file entries
#\$IMXE_DEFAULT: < Keyword=value>	#\$IMXE_DEFAULT: TYPE=router
For example: #\$IMXE_DEFAULT: TYPE=router	16.26.176.92 BldRtr6.compaq.com BldRtr6 #user comments

NOTE: If a keyword parameter is omitted on a commented entry, the current default value is used. The current default is always the standard default unless a new default value was set using the #\$IMXE_DEFAULT statement. Enclose keywords containing more than one word, such as "management processor." Enclose the full keyword in double quotation marks. Quotation marks are optional for single keywords like "server."

The following text quoted from a hosts file illustrates several statements. The explanations, which begin with the pound sign (#), are not displayed in the hosts file.

```
# Title: Systems in database
```

```
# Sorted by: IP address
# Date: 28-Mar-00 2:29:31 PM
# Author: administrator
```

The system EngProliant uses all current defaults. There are no additional comments.

```
16.26.176.92 EngProliant.compaq.com EngProliant #user comments
```

The system testServer in the following example defaults for TYPE. The defaults for SNMP Timeouts and Retries were restored for this system but only apply to testServer. The SNMP write community string default was changed and only applies to testServer.

```
#$IMXE: TYPE=Server
#$IMXE: SNMP_TIM=0 SNMP_RET=0 SNMP_MON=public
SNMP_CON=private
16.26.160.20 testServer.compaq.com testServer
```

All defaults in the following example for the system BldRtr1 are the same as for testServer, but had to be specified because they are not the global defaults. These changes apply only to BldRtr1.

```
#$IMXE: TYPE=Router
#$IMXE: SNMP_TIM=0 SNMP_RET=0 SNMP_MON=public
SNMP_CON=private
16.26.160.23 BldRtr1.compaq.com BldRtr1
```

For the system BldRtr5, the TYPE and protocols used for discovery were changed from the current defaults. Because the remaining keyword entries are missing, the standard defaults are applied for the SNMP timeouts, retries, and community strings.

```
#$IMXE: TYPE=Router
16.26.160.24 BldRtr5.compaq.com BldRtr5
```

For the system AcctServer, only the TYPE was changed from the current defaults.

```
#$IMXE: TYPE=Server
16.26.176.36 AcctServer.compaq.com AcctServer #user comments
```

The global default for TYPE was changed from Unknown to Router. All subsequent entries will be identified as routers until a TYPE statement is used to specify another type or restore the default.

```
#$IMXE_DEFAULT: TYPE=Router
16.25.176.38 FloorRtr2a.compaq.com FloorRtr2a #user comments
```

The default for the next host entry was changed to management processor, which is enclosed in quotes. #IMXE:
TYPE="Management Processor" AcctSvriLo.compaq.com
16.25.176.37 AcctSvriLo #user comments

...

Default values

If a parameter is missing in the hosts file, the default is applied. The following lists the parameters that can be used in hosts files:

Table 24 Hosts file default parameters

Keyword	Value	Description
TYPE	• Application • Cluster • Complex • Desktop • Enclosure • Environmental Monitor • Handheld • Hub • KVM Switch • Management Processor • Notebook • Partition • Power Distribution Unit • Power Supply • Printer • Rack • Resource Partition • Remote Access Device • Router • Server • Shared Resource Domain • Storage Device • Switch • Tape Library • Thin Client • UPS • Unknown • Unmanaged • Workstation	Unknown (Default)
SNMP	0 1	Disabled (Default) Enabled
HTTP	0 1	Disabled (Default) Enabled
SNMP_TIM	0 Greater than 0	System default (Default)
SNMP_RET	0 Greater than 0	System default (Default)

Table 24 Hosts file default parameters *(continued)*

Keyword	Value	Description
SNMP_MON	Public <Community String >	Read only (Default)
SNMP_CON	<Community String>	No default

To use a hosts file to specify systems for an automatic discovery, add the hosts file name to the **Ping inclusion ranges, system (hosts) names, templates, and/or hosts files** section of the **Discovery** page under the **Configure general settings** section. Enter the following statement: *\$Hosts_filename* where *Hosts_filename* is the name of the hosts file that you want to use.

H System Type Manager rules

System Type Manager enables you to extend HP SIM's SNMP-based discovery so that it is able to identify new types of systems. You do this by creating a System Type Manager rule that maps a System Object ID (OID), and optionally an additional [MIB](#) variable, to the desired type. Manufacturers assign unique System OIDs to their SNMP-instrumented products.

Systems supply information about themselves using variables described in files called MIBs. These values are enumerated using an industry-standard structure. MIBs are provided by vendors for their systems and must be registered with HP SIM to be accessible and usable from System Type Manager. HP preregisters all HP MIBs and many third-party MIBs. You can register the remaining MIBs using the MIB compiler, if you have the related systems on your network. If you examine a MIB, you will find modules, or groups of variables. Some variables have multiple values. Each of these values has an OID as well. You can use these OIDs to determine which system you have and its current behavior by querying these OIDs. For a list of default MIBs supplied by HP SIM, see [“Out-of-the-box MIB support in HP SIM”](#) (page 229).

You might need to enter a MIB variable OID if you have systems that return the same System OID that you would like to classify as different products based on an SNMP variable that returns a different value for each class. For example, if you have Windows NT servers from different vendors that return the same Windows NT System OID, you can specify rules using the Windows NT OID as the OID and a vendor-specific MIB variable and value combination to create separate rules for each vendor.

Adding new SNMP rules

You can create a new SNMP-based rule using the command line utility (`mxstm`) or by selecting **Options→Manage System Types** from the HP SIM user interface. Within the SNMP framework, manageable network systems (routers, bridges, servers, and so on) contain a software component called a *management agent*. The agent monitors the various subsystems of the network element and stores this information in a MIB. The agents enable the system to generate traps, which can be configured to be sent to a trap destination server that is running HP SIM.

I Custom tool definition files

Custom tool definition files are XML files that describe how HP SIM should run tasks based on a program, script, or UTL added by the user. This appendix describes the syntax of these tool definition files (tdef).

Tool type-specific requirements

SSA-specific attributes

An SSA tool executes on a selected target and is only aware of the target system environment. In executing an SSA tool, the HP SIM [Distributed Task Facility](#) (DTF) of the CMS uses SSH to send one or more files to the target system, which then executes the tool. An example of an SSA tool would be a tool that wraps a common Unix command such as **ls**, **cat**, or **cp**.

Table 25 SSA-specific attributes

Attribute	Syntax ¹	Description
ssa-block	<code><ssa-block> (<i>command/copy-block attributes</i>) </ssa-block></code>	You should specify only one command or copy-block or both; however, you may specify up to 16 multiple copy-blocks can be specified. After the command and/or copy-blocks, one may specify the parameters for the command and/or copy-block.
command	<code><command> (<i>parameters</i>) </command></code>	Specifies the command for an SSA tool. If the command accepts parameters, you must specify the command as a "Parameterized strings" (page 221). This element may have two attributes: command-type and log.
copy-block	<code><copy-block> (<i>attribute data</i>) </copy-block></code>	Specifies a source file path and a destination file path for a copy operation. The source element specifies the source file path for a copy operation. The destination element specifies the destination file path for a copy operation. The default permission of the copied block is 755. The <code>chmod</code> command is required to set a custom permission.

¹ Replace italicized text between start and stop tags with actual attribute/value/data. Non-italicized text represents valid entry option. You must specify values for attributes; there are no default values.

MSA-specific attributes

An MSA tool executes typically on the CMS and can work with multiple target systems. When launched, the MSA process is created once and then passed to all targets on the list. An XWindows tool is an example of an MSA tool.

MSA command tools must specify a command and the system on which the command will execute.

Table 26 MSA-specific attributes

Attribute	Syntax ¹	Description
msa-block	<code><msa-block></code> <i>(command/parameters)</i> <code></msa-block></code>	Specifies an MSA command, the parameters for the command, and an execution node on which the command executes.
command	<code><command></code> <i>(parameters)</i> <code></command></code>	Specifies the command for an MSA tool. If the command accepts parameters, you must specify the command as a “ Parameterized strings ” (page 221). This element may have two attributes: command-type and log.
Execution-node	<code><execution-node></code> <i>(parameters)</i> <code></execution-node></code>	

¹ Replace italicized text between start and stop tags with actual attribute/value/data. Non-italicized text represents valid entry option. You must specify values for attributes; there are no default values.

WLA-specific attributes

A WLA tool typically launches in a separate browser (by default) or in the same frame as HP SIM and is specified by a universal resource locator (URL). Web-launch applications that do not share HP SIM certificates should be executed in a separate frame.

Web-launch aware tools must specify a main URL.

Table 27 WLA-specific attributes

Attribute	Syntax ¹	Description
Web-block	<code><web-block></code> <i>(URL/format attributes)</i> <code></web-block></code>	Specifies a main-URL element. Also may specify parameters for the URLs. May optionally specify a target format to describe how targets are passed to a web launch aware tool.
Main-URL	<code><main-url></code> <i>http://xxx.xxx.xxx</i> <code></main-url></code>	A parameterized string defining the full URL that opens the main application window for this tool action. In the Portal UI this is considered the URL to display in the Work Window.
Side-URL	<code><side-url></code> <i>http://xxx.xxx.xxx</i> <code></side-url></code>	An optional, parameterized string defining the full URL that opens the small window view for this tool action. In the Portal UI this is considered the URL to display in the Set-Aside View Window.
Current-URL	<code><current-url></code> <i>http://xxx.xxx.xxx</i> <code></current-url></code>	An optional, parameterized string defining the full URL that is used to refresh the main application window for this tool action. In the Portal UI this is considered the URL to refresh the Work Window to maintain its current state.
Status-URL	<code><status-url></code> <i>http://xxx.xxx.xxx</i> <code></status-url></code>	An optional, parameterized string defining the full URL that opens a window to show on-going status for the Task ID associated with executing this tool. In the Portal UI this is considered the URL to display for the current status/results of the task when selecting the task from the Task Status List.

Table 27 WLA-specific attributes *(continued)*

Attribute	Syntax ¹	Description
Target-format	<target-format> <i>(parameters)</i> </target-format>	An optional parameterized string that provides a way for web-launch applications to pass long lists of targets. The <target-format> gets expanded in exactly the same manner as the URLs defined for the tool (for example, <main-url>).
System-page-link-group-title	<system-page-link-group-title> <i>(parameters)</i> </system-page-link-group-title>	Indicates the title of a section in the System Page Tools/Links tab. The content of this attribute is the displaying title for a section of links. For example, "Systems Insight Manager Pages" is a section title.

¹ Replace italicized text between start and stop tags with actual attribute/value/data. Non-italicized text represents valid entry option. You must specify values for attributes; there are no default values.

mxtool command parameters

The HP SIM `mxtool` command enables you to perform specific actions as defined by the parameter(s) that follow it. The following table is a partial list of common parameters used with the `mxtool` command.

Table 28 Command mxtool parameters

Parameter	Function
-a	Specify a file/tool to add
-d	Specify a directory
-f	Specify a file
-m	Modify/change
-r	Specify a file/tool to be removed
-t	Specify a tool name
-x force	Force a tool to be removed or modified even if the version is the same or tasks are tied to the tool

NOTE: For more information about `mxtool` parameters, refer to the `mxtool` man page in the HP SIM information library at the following URL: <http://www.hp.com/go/insightmanagement/sim/docs>, or in the *HP Systems Insight Manager Command Line Interface Guide*.

Parameterized strings

Parameterized strings allow tool developers to greatly enhance the options available in creating TDEFs. Parameterized strings contain replacement fields (similar to the format strings used in the popular `printf()` function in the standard C library). These fields can be replaced by values entered by the user at runtime (as defined by the tool parameters attribute), by some standard task properties supplied by the Task Controller by values related to the selected target systems or system groups, or by property values retrieved from a global tool properties file.

Parameterized string substitution descriptions

Table 29 Global attribute parameters

Parameter	Description
%t	Job ID for the task being executed
%u	Name of the user running this task
%e	Name of the user this task will execute as
%s	Management server hostname of the core CMS running the tool (the HP SIM server name)
%#	Substitute the value input by the user for the parameter referenced by the number (#) provided, as a list index position (one-based positive whole integer... %1, %2, %3, and so on). Up to 10 parameters are allowed, %A is used for the 10 th .
%y	SOAP logon token, for use with SOAP SSO Web applications

Table 30 Current selected target parameters

Parameter	Description
%f	The system name of the target system.
%n	Network name (hostname, IP address, IPX address, or system name in that order).
%a	Network address (IP address, or IPX address, in that order).
%l	Link name in format specified by System Link Configuration security setting (name, IP address, or full DNS name).
%p	IP address of WMI proxy, if any, for this target, in the form <ip address>:<port#></port#></ip>.
%g	HP SIM identifier or GUID of the target system.
%b	System type of the target system.
%c	System sub-type of the target system
%r% {rt[.attribute]%}	Substitutes the related system that has the relationship type as specified in the parameter rt. Valid relationship type strings are those that are stored in the associationTypeNumber column in the device_associations table. If the [.attribute] is specified, then one of the named system attributes would be returned for the related system. In addition, the common attributes such as Network name (.a) also work. For example, to get the IP address of the server's management processor, use %r%{MgmtProcToServer.a%}; to get the contact use %r%{MgmtProcToServer.Contact%}. If the related systems attribute is omitted, then for each system, the network name and IP address are returned in the form "network name ip address." If more than one system is returned, then they are comma-delimited. Note that the relationship type "MgmtProcToServer" can be used to return related system information for all management processor relationship types.
%{attribute}%}	The value of the named attribute of the target system.

Table 31 Multiple selected target parameters (not supported for Custom Command Tools)

Parameter	Description
%(... %)	Repeated pattern (only repeats if a current selection exists). If a current target selection does not exist, the text between the delimiters is removed on expansion. This allows the text to be optional and dependent upon the target selection list.
%i	Selection index (one-based).
%z	Do not substitute anything, but increment the selection index to the next integer and the referenced target system to the next target in the selected target list.
% < ... % >	Encrypted text (encrypt after all other parameters have been substituted).
%%	Enables you to retain a % in the command/URL after substitution.

NOTE: For more information about parameterized strings, refer to the HP SIM online help.

Common tool attributes

Common name values available to use for TDEFs.

Table 32 Task Wizard names values

Names values	Description
show-cmdline	Displays command line equivalent of GUI action. Values: True False (default: true)
Custom-page-n	Value is a string giving relative path to jsp page that should be displayed, where n = sequential value starting at 1.
ListType	Limits the types of selections available for choosing to only System Lists or only Event Lists. If this value is not present then both System and Events lists are available. Values: systemLists eventLists
SelectionType	Limits the type of selections allowed for the tool. If "list", then only lists (criteria) are allowed for selection. If "collection", then only collections (non-criteria) are allowed for selection. If "individual", then only individual systems are allowed for selection. Values: list individual collection
Targets-are-events	This informs the task wizard that the selections made for this tool are the actual events and not the systems from which the events were generated, which is the default behavior. When using this attribute, the task wizard will assume a "listType" of "eventLists" and a "selectionType" of "list".
PageIndex	By default, the task wizard displays the target selection page as the first page during task creation. When a tool defines its own custom parameter pages, they may instruct the task wizard where to place the target selection page. n = value starting at 1.
TargetSelection lockTargetSelection	A tool may wish to show the target selection page without allowing the user to change the target. Values: true false (default: false)

Table 33 Defined name values

Names values	Description
product-name	32 character string
Product-version	24 character number
Insert-separator	Insert a separator line in the menu structure before ("true") or after ("after") this tool. Values: true after false (default: false)
l18n-attribs	String. Name of a resource bundle for storing localized tool parameters. See the section on tool internationalization.
Tool-id	String. Normally, the portal will refer internally to the tool using its database GUID. If a tool needs a well-known ID that will not change, this attribute can be used.
Show-selections	Have the portal show—in the workspace—the number of selected nodes, linked to a popup window that displays a list of selected nodes. Values: true false (default: false)
help-url	String. Set this URL as the portal's current help URL when this tool loads. The help URL will be loaded into a separate browser window, and the name of the browser frame will be "helpWindow".

Table 34 All tools values

Names values	Description
show-snap-off	Have the portal provide a hyperlink for tool's workspace to be snapped off into a separate browser window. Values: true false (default: false)
menu-path	A string in the form "base submenu subsubmenu". Overrides the tool's category.
title	String. Display the supplied string in the tool's window title area. By default, the name of the tool (used in the Manage menu) will be used as the title of the tool.
show-title	Values: true false. (default: true) If false, the portal will not display a title bar for the tool.
Menu-sort-key	String. Integer sort key used to sort among the other menu items in the group. The lower the number, the earlier the item appears in the menu. If a group of menus consists of menus without sort keys, then those without keys are sorted alphabetically and put at the end
Trail-blazer	A trailblazer is a definition used only to establish the presence of cascades in the menu system and to apply a sorting order to them. Values: true false (default: false)

Table 35 Web-launch tools

Names values	Description
Target-frame	String. Indicates not to load the tool's URL into a workspace; instead, load the URL into the specified frame.

Tool Filtering attributes

Common filtering values available to use for TDEFs.

Table 36 Tool filtering attributes

Filter name	Description
OSName	Acceptable values include: HPUX (no space or hyphen in the value) Linux WINNT (all windows flavors) VMware ESX
OSVendor	Acceptable values include: Microsoft SuSE RedHat HP
OSRevision	Acceptable values are as follows (see text below for version number details) (for Windows) 5.2, 6.0, 6.1 (for Linux) 3, 4, 4.1, 5.5, 10.2, 11 (for HP-UX) 11.31
DeviceType	Long list: Bring up the Options menu, then select Discovery and then Identification . Select Manage System Types to see the list.
DeviceSubtype	Long list: Bring up the Options menu, then select Discovery and then Identification . Select Manage System Types to see the list.
Protocol	Acceptable values are as follows (see text below for version details) SNMP: 1.0 WBEM: 1.1 SMH: 1.0 or 2.0 (This is the System Management Homepage running on a device) SSH:

The OSRevision and Protocol Support node attributes have values that are interpreted as version numbers. A version number is a series of non-negative decimal numbers separated by period (.) characters. When comparing version numbers, the following rules are used:

- The leftmost numbers in the series are most significant, so "1.0" is greater than "0.1".
- Leading zeroes on the numbers are disregarded, so "003" is equal to "3".
- Two adjacent period characters are interpreted as if they delimited the number zero, so "1.0.3" is equal to "1..3".
- A beginning period character is interpreted as if preceded by a zero, so ".9" is equal to "0.9".
- Trailing zero numbers are disregarded, so "1.0.0" is equal to "1"

Environment Variables

Specific environment variables (EVs) available to use for TDEFs. In addition to this list, operating system environment variables are also available (for Windows systems) to be passed into TDEFs.

In addition to these "automatic" EV's, user-defined environment variables may be set as part of scripting in the TDEFs.

Table 37 Environment Variables

Names values	Description
NoticeLabel	The short string type of event (like Discovered Device)
NoticeState	Shows whether the event has been cleared
NoticePlainText	Plain text description of the event and also includes whether it is set to In Progress, Cleared, or Not Cleared
NoticeRawData	The raw data of the event that was sent and in a string format. It is in a pipe () delimited format that can be used for simple parsing
NoticeSeverityStr	Can be Critical, Major, Minor, Unknown, Normal, Warning, or Informational
NoticeSeverity	An integer format of the severity 1 – Normal 2 – Warning 3 – Minor 4 – Major 5 – Critical 6 – Informational
NoticeQueryName	Displays the event list that generated the event. In the format of: • This device or event meets the following query criteria: +QueryName ; • This device or event now meets the following query criteria: +QueryName ; • This device or event no longer meets the following query criteria: QueryName
DeviceName	Name of the device that generated the event
DeviceIpxAddressCount	Number of IPX addresses that are mapped to this device
DeviceIPAddressCount	Number of IP addresses that are mapped to this device
DeviceIPAddress%d	Based on the count of IP addresses, %d is an integer that shows the actual IP address. For example, if DeviceIPAddressCount=2 then DeviceIPAddress0=111.111.111.111 and DeviceIPAddress1=222.222.222.222.
DeviceMACAddress%d	Based on the MAC address count, %d is an integer that references the actual MAC address variable. If DeviceMACAddressCount=2 then, DeviceMACAddress0=00:80:5E:7F:B0:81 and DeviceMACAddress1=00:80:C7:29:EF:B6
GenericTrapID	If tied to an event list and the event was a SNMP trap, then this is set to the SNMP generic trap ID of the trap received
SpecificTrapID	If tied to an event list and the event was a SNMP trap, then it is set to the SNMP specific trap ID

Table 37 Environment Variables *(continued)*

Names values	Description
Path	Path variable received from the operating system (received in context of the windows service account)
SystemRoot	Variable received from the operating system (received in context of the windows service account)
WinDIR	Variable received from the operating system (received in context of the windows service account)
ComputerName	Variable received from the operating system (received in context of the windows service account)

Tool parameter guidelines

Guidelines for entering parameter field data when creating new command line tools.

Table 38 New Command Line Tool parameter entry guidelines

Parameter field	Data entry required?	Parameter string assignment	Entry guidelines
Tool name	Yes	%1	As when using the CLI, the name of the new tool should be descriptive of the tool's function.
Tool command	Yes	%2	This is the new command used to call the tool, and it may include parameters.
Prompt	No	%3	If the Tool command includes the %1 parameter, then this field entry is required to specify the destination prompt.
Tool menu category	No	%4	Use this entry to specify the location of the tool in the menu. If left blank, the new tool will be added to the Tools→Command Line Tools menu.
Tool description	No	%5	Description of what the new tool does.
Tool help comment	No	%6	Description of how to use (invoke) the new tool.
Enter <code>root</code> execute as root	No	%7	If left blank, the new tool will run as the HP SIM user whose SSH public key must be configured on the managed system using the <code>mxagentconfig</code> command. Refer to the HP SIM Installation and User Guide for more information. CAUTION! If <code>root</code> is specified, any user authorized to run this tool may gain full access to the managed system depending on the definition of the

Table 38 New Command Line Tool parameter entry guidelines *(continued)*

Parameter field	Data entry required?	Parameter string assignment	Entry guidelines
			command and its capabilities.
File path to save tool	No	%8	Path name of new tool. Example: /var/opt/mx/ tools/mytool.xml

J Out-of-the-box MIB support in HP SIM

The following table represents the key MIBs that ship with HP SIM. Those MIBs that are marked as preloaded are registered as part of every HP SIM installation. The remaining MIBs are in the MIB directory for you to compile, if necessary, for managing those types of systems in your environment.

Table 39 MIBs supported in HP SIM

MIB name	Supports	Pre-loaded
asmib.mib	ARC Serve	X
atmf.mib	ATM device	X
avsnmpv1.mib	Availant Manager	X
bkupexec.mib	General Backup	X
bladetype2-network.mib	HP ProLiant BL p-Class GbE2 Interconnect Switch	X
bladetype2-physical.mib	HP ProLiant BL p-Class GbE2 Interconnect Switch	X
bladetype2-switch.mib	HP ProLiant BL p-Class GbE2 Interconnect Switch	X
bladetype2-trap.mib	ProLiant BL P-class GbE2 Interconnect Switch	X
bladetype4-switch.mib	hpSwitchProLiant	
bridge.mib	Cisco bridge	X
cisco-cdp.mib	cisco products	X
cisco-cluster.mib	cisco products	X
cisco-config-copy.mib	cisco products	X
cisco-config-man.mib	cisco products	X
cisco-entity-fru-control.mib	cisco products	X
cisco-entity-vendortype-oid.mib	cisco products	X
cisco-envmon.mib	cisco products	X
cisco-flash.mib	cisco products	X
cisco-ftp-client.mib	cisco products	X
cisco-igmp-filter.mib	cisco products	X
cisco-image.mib	cisco products	X
cisco-ip-stat.mib	cisco products	X
cisco-l2l3-interface-config.mib	cisco products	X
cisco-lag.mib	cisco products	X
cisco-mac-notification.mib	cisco products	X
cisco-memory-pool.mib	cisco products	X
cisco-pae.mib	cisco products	X
cisco-pagp.mib	cisco products	X
cisco-ping.mib	cisco products	X

Table 39 MIBs supported in HP SIM (continued)

MIB name	Supports	Pre-loaded
cisco-port-security-mib.mib	cisco products	X
cisco-process.mib	cisco products	X
cisco-products.mib	cisco products	X
cisco-rttmon.mib	cisco products	X
cisco-stack-mib.mib	cisco products	X
cisco-stackmaker.mib	cisco products	X
cisco-stp-extensions.mib	cisco products	X
cisco-syslog.mib	cisco products	X
cisco-tc.mib	cisco products	X
cisco-tcp.mib	cisco products	X
cisco-udldp.mib	cisco products	X
cisco-vlan-iftable-relationship.mib	cisco products	X
cisco-vlan-membership.mib	cisco products	X
cisco-vtp.mib	cisco products	X
compaq-agent.mib	HP Rack and Enclosure	X
compaq-id-rec.mib	HP ProLiant BL pClass GbE series Product	X
cpq-traps.mib	HP ProLiant BL P-class GbE Interconnect Switch	X
cpq54nn.mib	Giga Switch	X
cpqclus.mib	HP ProLiant Cluster	X
cpqcmc.mib	HP ProLiant remote management	X
cpqcr.mib	HP ProLiant Cluster	X
cpqdsccs.mib	Cpqdsccs	X
cpqfca.mib	HP ProLiant Storage	X
cpqgen.mib	HP ProLiant Miscellaneous	X
cpqhlth.mib	HP ProLiant System and Environmental	X
cpqhost.mib	HP ProLiant Application	X
cpqida.mib	HP ProLiant Storage	X
cpqide.mib	HP ProLiant Storage	X
cpqidrec.mib	HP proLiant BL pClass GbE Device	X
cpqn5226a.mib	Giga Switch	X
cpqnic.mib	HP ProLiant NIC	X
cpqpower.mib Power	Device	X
cpqrack.mib	HP ProLiant Rack	X
cpqrecov.mib	HP ProLiant Cluster	X
cpqrpm.mib	HP ProLiant UPS	X

Table 39 MIBs supported in HP SIM *(continued)*

MIB name	Supports	Pre-loaded
cpqsanapp.mib	SAN Appliance	X
cpqsanevent.mib	SAN Appliance	X
cpqscsi.mib	HP Proliant Storage	X
cpqservice.mib	HP Service	X
cpqsinfo.mib	HP Proliant System and Environmental	X
cpqsm2.mib	HP Proliant remote management	X
cpqsrvmn.mib	HP Proliant System and Environmental	X
cpqstdeq.mib	HP Proliant System and Environmental	X
cpqstsys.mib	HP Proliant Storage	X
cpqthrsh.mib	HP Proliant threshold	X
cpqups.mib	HP Proliant UPS	X
cpqwcrm.mib	System and Environmental	X
cpqwinos.mib	HP Proliant Operating System	X
dataprotector.mib	Data protector	X
dlghwinf.mib	Dialogic Hardware	X
ems.mib	HP-UX EMS	X
emsmibax.mib	Tandem EMS	X
fddi-sm73.mib	FDDI subsystems	X
fe-mib.mib	Fibre Channel Fabric Element	X
gbe2c-10g-l2l3.mib	hpProliant-GbE2c-10G-InterconnectSwitch	
gbe2c-10g-l2l3.mib	hpProliant-GbE2c-10G-InterconnectSwitch	
hp-mccluster.mib	HP Serviceguard	X
hp-switch-pl.mib	HP Blade Network switch	X
hpeccmib.mib	NetServer	X
hpi02trap.mib	HP Integrity Server	X
hpi02trap.mib	HP Integrity Server	X
hpn.mib	NetServer	X
hpnetctz.mib	CommandView	X
hpnr.mib	NetServer	X
hpov-nnm.mib	HPOV	X
hpovsam.mib	HP OVSAM	X
hpovsam_im.mib	HP STORAGE	X
hprfrmib.mib	HP Netserver	X
hpsgcluster.mib	HP ServiceGuard	X
hpswa.mib	HP Netserver	X
hptat.mib	HP Netserver	X

Table 39 MIBs supported in HP SIM *(continued)*

MIB name	Supports	Pre-loaded
hs_agent.mib	SWCC	X
lsf001.mib	LSF product	X
msa2000traps.mib	MSA2000 Array(HPMSA)	X
nsadimm.mib	HP Netserver	X
nsaevent.mib	HP Netserver	X
nsainfo.mib	HP Netserver	X
nsapci.mib	HP Netserver	X
nsascsi.mib	HP Netserver	X
nsavolcp.mib	HP Netserver	X
old-cisco-chassis.mib	cisco products	X
old-cisco-flash.mib	cisco products	X
old-cisco-interfaces.mib	cisco products	X
old-cisco-ip.mib	cisco products	X
old-cisco-sys.mib	cisco products	X
old-cisco-tcp.mib	cisco products	X
old-cisco-ts.mib	cisco products	X
ovis-v2.mib	HP Open View Internet Services	X
pcisnet.mib	ServerNet	X
pfc.mib	PATROL	X
rfc1213.mib	RFC MIB	X
rfc1215.mib	RFC MIB	X
rfc1514.mib	RFC MIB	X
rmon-mib.mib	RFC MIB	X
smsagent.mib	Unisys Configuration Agent	X
svrclu.mib	Common Cluster	X
switch.mib	ServerNet	X
symtrap.mib	Integrity Server	X
truclu.mib	TruCluster	X
ucd-snmp-mib.mib	Numerical Management	X
v5_0ficon.mib	FICON in Fabos	X
v5_1ha.mib	Brocade Communications Systems	X
v5_3sw.mib	Fibre Channel Switch	X
wbt3mib.mib	WYSE Events	X
xp1024trapmib.mib	Hitachi RAID450 SNMP Agent	X
zesa.mib	ZESA	X
zhrm.mib	ZHRM	X

Table 39 MIBs supported in HP SIM *(continued)*

MIB name	Supports	Pre-loaded
zsmplib	Tandem's Subsystem Control Facility (SCF)	X
zlmplib	Tandem SNMP Trap Multiplexer	X
ztsa.mib	Tandem TCP/IP Subagent	X

K Support and other resources

Information to collect before contacting HP

Be sure to have the following information available before you contact HP:

- Software product name
- Hardware product model number
- Operating system type and version
- Applicable error message
- Third-party hardware or software
- Technical support registration number (if applicable)

How to contact HP

Use the following methods to contact HP technical support:

- In the United States, see the Customer Service/Contact HP United States website for contact questions:
http://welcome.hp.com/country/us/en/contact_us.html
- In the United States, call +1 800 334 5144 to contact HP by telephone. This service is available 24 hours a day, 7 days a week. For continuous quality improvement, conversations might be recorded or monitored.
- In other locations, see Contact HP Worldwide website for contact options:
<http://welcome.hp.com/country/us/en/wwcontact.html>

Security bulletin and alert policy for non-HP owned software components

Open source software (such as OpenSSL) or third-party software (such as Java) are sometimes included in HP products. HP discloses that the non-HP owned software components listed in the Insight Management end user license agreement (EULA) are included with Insight Management. The EULA is included with the Insight Management Installer on Insight Management DVD #1.

HP addresses security bulletins for the software components listed in the EULA with the same level of support afforded HP products. HP is committed to reducing security defects and helping you mitigate the risks associated with security defects when they do occur.

When a security defect is found, HP has a well defined process that culminates with the publication of a security bulletin. The security bulletin provides you with a high level description of the problem and explains how to mitigate the security defect.

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

http://www.hp.com/country/us/en/contact_us.html

After registering, you will receive email notification of product enhancements, new driver versions, firmware updates, and other product resources.

Registering for software technical support and update service

HP SIM is supported in any one of the following situations:

- A valid warranty exists (90 days Global Limited Warranty)
- Purchase of Insight Control (having 1-year 24x7 Technical Support bundled with the license purchase)

- If the question is related to HP Insight Remote Support (HP Insight RS), then HP SIM will be supported as it pertains in Insight RS with a Hardware Warranty or Hardware Contract
- The customer purchases an HP SIM Care Pack (Part #: UR389E)

Support includes one year of 24 x 7 HP Software Technical Support and Update Service. This service provides access to HP technical resources for assistance in resolving software implementation or operations problems.

The service also provides access to software updates and reference manuals in electronic form as they are made available from HP.

With this service, customers benefit from expedited problem resolution as well as proactive notification and delivery of software updates. For more information about this service, see the following website:

<http://www.hp.com/services/insight>

Registration for this service takes place following online redemption of the license certificate.

How to use your software technical support and update service

As HP releases updates to software, the latest versions of the software and documentation are made available to you. The Software Updates and Licensing portal gives you access to software, documentation and license updates for products on your HP software support agreement.

You can access this portal from the HP Support Center:

<http://www.hp.com/go/hpsc>

After creating your profile and linking your support agreements to your profile, see the Software Updates and Licensing portal at <http://www.hp.com/go/hpsoftwareupdatesupport> to obtain software, documentation, and license updates.

HP authorized resellers

For the name of the nearest HP authorized reseller, see the following sources:

- In the United States, see the HP U.S. service locator website:
http://www.hp.com/service_locator
- In other locations, see the Contact HP worldwide website:
<http://www.hp.com/go/assistance>

Related documents

Documentation and support

For support, software updates, and additional information on HP SIM and other products used with HP SIM, see the following websites:

- HP SIM website at <http://www.hp.com/go/hpsim/> for general product information and links to software downloads, documentation, and troubleshooting information
- HP Software Depot website at <http://www.software.hp.com/> for access to HP SIM software downloads
- HP Business Support Center website at <http://www.hp.com/bizsupport/> for support information about HP SIM and HP Commercial products
- HP Support Center website at <http://www.hp.com/go/hpsc> for support information about HP SIM and HP Enterprise products
- HP SIM SMI-S Providers website at <http://www.hp.com/go/hpsim/providers> for information about device support and SMI-S providers
- Videos that showcase HP SIM and the Essentials at
- HP SIM forum at http://h18013.www1.hp.com/products/servers/management/hpsim/techsupport.html?jumpid=hpr_r1002_usen_link1 for discussions about HP SIM

HP SIM documentation

For more information regarding HP SIM, see the HP HP SIM Information library at <http://www.hp.com/go/insightmanagement/sim/docs> for access to HP SIM manuals and release notes.

Typographic conventions

<code>find(1)</code>	HP-UX manpage. In this example, “find” is the manpage name and “1” is the manpage section.
<i>Book Title</i>	Title of a book or other document.
<u>Linked Title</u>	Title that is a hyperlink to a book or other document.
<u>http://www.hp.com</u>	A Web site address that is a hyperlink to the site.
Command	Command name or qualified command phrase.
user input	Commands and other text that you type.
computer output	Text displayed by the computer.
Enter	The name of a keyboard key. Note that Return and Enter both refer to the same key. A sequence such as Ctrl+A indicates that you must hold down the key labeled Ctrl while pressing the A key.
term	Defined use of an important word or phrase.
variable	The name of an environment variable, for example PATH or errno.
value	A value that you may replace in a command or function, or information in a display that represents several possible values.
<element>	An element used in a markup language.
attrib	An attribute used in a markup language.

Documentation feedback

HP is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hp.com). Include the document title and part number, version number, or the URL when submitting your feedback.

Glossary

A

administrative rights user	A user who is authorized for the All Tools toolbox on all systems, including the CMS. This type of user has been given special privileges to administer the HP SIM software.
administrator	A user who manages users, resource pools, and self-service requests through HP Insight Orchestration console.
agent	A program that regularly gathers information or performs some other service without the user's immediate presence. HP SIM agents provide in-depth hardware and software information and subsystem status to HP SIM and numerous third-party management applications. <i>See also</i> management agent.
alarm	A user-configurable notification displayed in the System Status panel of HP SIM when certain events occur. For instance, if a monitored item changes, an alarm notifies the user that a change has occurred. <i>See also</i> trap, event.
all events collection	Displays all events that have occurred for all systems.
All Tools toolbox	A default toolbox that provides complete access to all tools for the authorized system or system group.
authentication	The process of identifying an individual, based on a user name and password. Authentication is distinct from authorizations and ensures that the individual is who they claim to be.
authorizations	A mapping of a relationship between a user, a toolbox, and a system or system group.
automatic discovery	The process that HP SIM uses to find and identify systems on your network and populate the database with that information. A system must first be discovered to collect data and track system health status. The primary source for automatic discovery is ping sweeps configured in the automatic discovery tasks page. Other sources might include receiving events from unknown systems or from a management processor that has information about a server. Identification automatically runs on discovered systems.
available software	A listing of the software components available in the repository to which the Version Control Agent (HP VCA) has been configured to point. When browsing directly into a HP VCA, these additional components can be selected for installation.

B

banner	The section of the GUI at the top of the screen that includes the user name and links to the Home page and sign out functions.
---------------	---

C

caution	A note to indicate that failure to follow directions could result in damage to equipment or loss of information.
central processing unit polling rate	The rate for how often the Cluster Monitor CPU Resource checks CPU utilization as reported by Insight Management Agent on monitored systems.
certificate	An electronic document that contains a subject's public key and identifying information about the subject. The certificate is signed by a certificate authority (CA) to bind the key and subject identification together. <i>See also</i> certificate authority.
certificate authority	A trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. The role of the CA in this process is to guarantee that the individual who has been granted the unique certificate is the individual they claim to be.
cleared status	A status condition that indicates an event is cleared.
clients	HP desktop, portable, and workstation systems.

cluster	A parallel or distributed computing system made up of many discrete systems that form a single, unified computing resource. Clusters vary in their features, complexity, and the purposes for which they are best suited.
cluster monitor resource	A program that provides a monitoring or management function for clustered nodes in a cluster.
CMS	A system in the management domain that executes the HP SIM software. All central operations within HP SIM are initiated from this system.
collections	The method for grouping system or event.
command line interface	A text-based application that can be executed from a command shell such as sh, csh, ksh or the Microsoft Windows CMD shell.
common information model	An object-oriented schema defined by the Desktop Management Task Force (DMTF). CIM is an information model guide that describes and shares management information enterprise-wide. CIM is designed for extending each management environment in which it is used.
common information model object manager	A CIMOM acts as the interface for communication between web-based enterprise management (WBEM) providers and management applications such as HP Systems Insight Manager. A CIMOM that provides an interface for an SMI-S provider is called an SMI CIMOM.
communications protocol	See management protocol.
complex	Computer systems that support multiple hardware partitions are referred to as a complex. For example, the HP Integrity Superdome systems support multiple hardware partitions within a single complex.
component	A component is a single, self-describing, installable (interactive or silent) binary file containing a single piece of software, such as firmware image, driver, agent, or utility, that is supported by the management and update tools.
Configure or Repair Agents	An HP SIM feature that enables you to repair credentials for SNMP settings and trust relationships that exist between HP SIM and target systems. You can also update Web Agent passwords on target systems that have 7.1 agents or earlier installed.
critical status	A state generated when HP SIM can no longer communicate with a managed system.
Cygwin	A UNIX compatibility layer that is used to port some UNIX utilities to Windows.

D

data collection tasks	Procedure that involves gathering information from a group of managed systems and storing that information in the database. HP SIM uses Hardware Status Polling and Data Collection Tasks to implement data collection.
digital signatures	A technology used to validate the sender of a transaction. This technology uses private keys to digitally sign the data and public keys to verify the sender.
discovery	A feature within a management application that finds and identifies network objects. In HP management applications, discovery finds and identifies all the HP systems within a specified network range.
discovery filters	Enables users with to prevent or allow certain system types from ever being added to the database.
Distributed Component Object Model	An extension of the Component Object Model (COM) that enables COM components to communicate between clients and servers on the same network.
Distributed Task Facility	A management application that manages the remote execution of tasks on managed systems.
Domain Name Service	A service that translates domain names into IP addresses.

E

enclosure	A physical container for a set of server blades. It consists of a backplane that routes power and communication signals and additional hardware for cabling and thermal issues. It also hosts the CPU or server power supplies.
------------------	---

event	Information sent to certain users that something in the managed environment has changed. Events are generated from SNMP traps. HP SIM receives a trap when an important event occurs. Events are defined as: • Warning. Events of this type indicate a state that might become a problem. • Informational. Events of this type require no attention and are provided as useful information. • Normal. Events of this type indicate that this event is not a problem. • Minor. Events of this type indicate a warning condition that can escalate into a more serious problem. • Major. Events of this type indicate an impending failure. • Critical. Events of this type indicate a failure and signal the need for immediate attention.
--------------	---

G

graphical user interface	A program interface that takes advantage of the graphics capabilities of the computer to make the program easier to use. The HP SIM GUI runs in a web browser.
---------------------------------	--

H

health status	Health status is an aggregate status all of the status sources (which can be SNMP, WBEM, and HTTP) with the most critical status being displayed. See also system health status.
host key	The public key that proves the identity of a particular host.
hosts files	A file that follows the UNIX, Linux, or Windows host file format, which is an IP address followed by a name and each system is listed on a separate line in this file. This file is used by discovery to manually add multiple systems to the HP SIM database,
HP Version Control Agent	The all-in-one vulnerability assessment and patch management tool integrated into HP SIM, simplifying and consolidating the proactive identification and resolution of issues that can impact server availability into one central console.
HyperText Transfer Protocol	The underlying protocol used by the World Wide Web.
Insight Control power management	An integrated power monitoring and management application that provides centralized control of server power consumption and thermal output at the datacenter level. It extends the capacity of datacenters by enabling the user to control the amount of power and cooling required for ProLiant servers. Built on ProLiant Power Regulator Technology, it extends new server energy instrumentation levers into HP SIM for greater Unified Infrastructure Management.
Insight Control virtual machine management	Provides central management and control of Virtual Machines on Microsoft Virtual server, Vmware's GSX and ESX. Integrated with HP SIM, virt provides unified management of HP ProLiant host servers and virtual machines.
Insight Management Advisor	A program that regularly gathers information or performs some other service without the user's immediate presence.
Systems Insight Manager	System management software that is capable of managing a wide variety of systems, including HP systems, clusters, desktops, workstations, and portables. HP SIM combines the strengths of Insight Manager 7, HP Tootools, and HP Servicecontrol Manager to deliver a single tool for managing HP ProLiant, Integrity, and HP 9000 systems running Windows, Linux, and HP-UX. The core HP SIM software delivers the essential capabilities required

to manage all HP server platforms. HP SIM can also be extended to deliver unparalleled breadth of system management with plug-ins for HP storage, power, client, and printer products. Plug-ins for rapid deployment, performance management, and workload management enable systems administrators to pick the value added software required to deliver complete lifecycle management of their hardware assets.

Systems Insight Manager database	The database that stores vital information about HP SIM, including users, systems, and toolboxes.
Version Control Agent	An agent that is installed on a server to enable you to see the HP software installed on that server. The HP VCA can be configured to point to Version Control Repository Manager, enabling easy version comparison and software update from the repository.
Version Control Repository Manager	An HP agent that enables a customer to manage HP provided software stored in a user-defined repository.
I	
identification	While discovery finds systems, identification attempts to determine what the system type is. In addition, it determines what management protocol a system supports, using credentials from the Global Protocol Settings page, and attempts to determine the operating system and version loaded, along with other basic attributes about the system. Finally, it determines if the system is associated with another system. For example, a management processor in a server.
installed version	A particular HP software component that is installed on the server.
Internet Engineering Task Force	From the IETF Web page: "The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet."€
Internet Protocol	Specifies the format of datagrams (packets) and the addressing scheme on a network. Most networks combine IP with Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source.
IP range	Systems with an IP address that falls in the specified range.
J	
Java Remote Method Invocation	A set of protocols that enable Java objects to communicate remotely with other Java objects.
M	
Major status	Status information collected from the system that indicates one or more of the monitored subsystems are not operating properly which is impacting the system. Action should be taken immediately.
managed systems	Any system managed by HP SIM, such as servers, desktops, storage systems, and Remote Insight Boards (RIBs).
management agent	A daemon or process running on a managed system. It receives and executes requests from the CMS on the managed system.
management domain	A collection of resources called managed systems that have been placed under the control of HP SIM. Each CMS is responsible for a management domain. The managed systems can belong to more than one management domain.
Management HTTP Server	An integrated piece of software used by the HP suite of HP Web-enabled System Management Software to communicate over HTTP and HTTPS. It provides a uniform set of functionality and security to HP Web-enabled System Management Software. This version is available in the ProLiant Support Pack.10 or earlier.
Management Information Base	The data specification for passing information using the SNMP protocol. An MIB is also a database of managed objects accessed by network management protocols.
management instrumentation	Agents running on systems that provide management information for HTTP, or SNMP protocols.

management protocol	A set of protocols, such as WBEM, HTTP, or SNMP, used to establish communication with discovered systems.
Minor status	Status information collected from the system that indicates one or more of the monitored subsystems are not operating properly which is impacting the system. Action should be taken as soon as possible to prevent further failure.
Monitor Tools toolbox	A default toolbox that contains tools that display the state of managed systems but not tools that change the state of managed systems.
multiple-system aware tool	A run type that supports multi-system operations. Tools with this run type operate on the target systems using their own internal mechanisms instead of using the Distributed Task Facility. The MSA run type uses the Distributed Task Facility to launch the tool on a single system before the tool interacting with the other managed systems.

O

Onboard Administrator	The Onboard Administrator is the central point for controlling an entire c-Class enclosure. It offers configuration, power, and administrative control over the rack, and its associated blades (Compute Servers), blade management processors (iLOs), network switches (depending on the models of switches used) and storage components (such as SAN or SATA). The Onboard Administrator is a single management processor, with shared resources to an optional backup twin processor for failover.
OpenSSH	A set of network connectivity tools providing encrypted communication sessions over a computer network using SSH. It was created as an open source alternative to the proprietary SSH software suite offered by SSH Communications Security.
operator rights user	A user who has limited capability to configure the CMS. operator rights users have permission to create, modify, and delete all reports and their own tools.
overall software status	This section indicates whether the software on the server that the HP VCA is installed on has any updates available within the repository in which it has been configured to monitor.

P

HP Insight Control performance management	A software solution that detects, analyzes, and explains hardware bottlenecks on HP ProLiant servers. performance management tools consist of Online Analysis, Offline Analysis, Comma Separated Value (CSV) File Generator Report, System Summary Report, Status Analysis Report, Configuration, Licensing, and Manual Log Purge.
Predefined private key	Reports that have been defined and installed with HP SIM. the private half of a public and private key pair. The private key is stored in and owner read-only file (for example, only the owner can view it) on a particular system. The private key is never transmitted to another system.
ProLiant and Integrity Support Packs	An ProLiant and Integrity Support Packs is a set of HP software components that have been bundled together by HP, and verified to work with a particular operating system. An ProLiant and Integrity Support Packs contains driver components, agent components, and application and utility components. All of these are verified to install together.
ProLiant Essentials license key	The contractual permissions granted by HP to the customer in the form of a coded embodiment of a license that represents a specific instance of a license. A single license can be represented by a single key or by a collection of keys.
ProLiant Support Pack	A set of HP software components that have been bundled together by HP and verified to work with a particular operating system. A ProLiant Support Pack contains driver components, agent components, and application and utility components. All of these are verified to install together.
public key	the public half of a public and private key pair. The public key can be freely distributed without fear that it can be used to impersonate the user. It can only be used for authentication in conjunction with a private key.

R

HP Insight Control server deployment	The HP Insight Control server deployment is a multiserver deployment tool that enables IT administrators to easily deploy large numbers of servers in an unattended, automated fashion.
---	---

The server deployment is installed separately from HP SIM. It requires a license for each server managed. You must register your server deployment product to purchase licenses. See the server deployment documentation for network environment setup, prerequisites for the deployment server, and installation instructions.

HP Insight Control server provisioning	HP Insight Control includes the rights for Insight Control server provisioning, which is a new feature replacing HP Insight Control server deployment. Insight Control server provisioning performs multi-server operating system provisioning to bare metal ProLiant and BladeSystem servers. You can download the Insight Control server provisioning installation instructions from http://www.hp.com/go/insightcontrol/docs .
HP Insight Remote Support Pack	The HP Insight Remote Support Pack provides proactive remote monitoring, diagnostics, and troubleshooting to help improve the availability of HP-supported servers and storage devices in your data center. The Remote Support Pack reduces cost and complexity in support of systems and devices. The Remote Support Pack securely communicates incident information through your firewall and/or Web proxy to the HP Support Center for reactive support. Additionally, based on your support agreement, system information can be collected for proactive analysis and services.
rack	A set of components cabled together to communicate between themselves. A rack is a container for an enclosure.
Red Hat Package Manager	The Red Hat Package Manager is a powerful package manager that can be used to build, install, query, verify, update, and uninstall individual software packages. A package consists of an archive of files and package information, including name, version, and description.
Replicate Agent Settings	A tool that can be used to copy web-based agent settings to a group of systems.
repository	A directory containing ProLiant and Integrity Support Packs and Smart Components.
Resource Partition	A subset of the resources owned by an operating system instance. The use of those resources is controlled through technologies such as the Fair Share Scheduler, pSets, and Memory Resource Groups. A resource partition also has a set of processes associated with it, and only those processes can use the resources within the resource partition. Policies established by tools such as Process Resource Manager (PRM), Workload Manager (WLM), or Global Workload Manager (gWLM) control how resources are allocated to the set of resource partitions within an operating system instance.
role	See toolbox.
S	
SAN	A storage area network (SAN) is a network (or subnetwork) that connects data storage devices with associated data servers. A storage area network is typically part of an overall network of computing resources.
search criteria	A set of variables (information) used to define a requested subset of information from the HP SIM database.
Secure HTTP	An extension to the HTTP protocol that supports sending data securely over the web.
Secure Shell	A program to log in to another system over a network and execute commands on that system. It also enables you to move files from one system to another, and it provides authentication and secure communications over insecure channels.
Secure Sockets Layer	A standard protocol layer that lies between HTTP and TCP and provides privacy and message integrity between a client and server. A common usage of SSL is to provide authentication of the server, so clients can be assured they are communicating with the server it claims to be. It is application protocol independent.
Secure Task Execution	A feature of HP SIM that securely executes a task from a managed system. STE ensures that the user requesting the task has the appropriate rights to perform the task, and encrypts the request to protect data from snooping.
server blade	Typically a very dense server system containing microprocessors, memory, and network connections that can be easily inserted into a rack-mountable enclosure to share power supplies, fans, switches,

and other components with other server blades. Server blades tend to be more cost-efficient, faster to deploy, and easier to adapt to growth and change than traditional rack-mounted or tower servers.

See also enclosure.

Shared Resource Domain

A collection of compartments—all of the same type—that share system resources. The compartments can be nPartitions, virtual partitions, processor sets (pSets), or Fair Share Scheduler (FSS) groups. A server containing nPartitions can be an SRD—as long as nPartition requirements are met. A server or an nPartition divided into virtual partitions can be an SRD for its virtual partition compartments. Similarly, a server, an nPartition, or a virtual partition containing pSets can be an SRD for its pset compartments. Lastly, a Server, an nPartition, or a virtual partition containing FSS groups can be an SRD for its FSS group compartments.

A complex with nPartitions can hold multiple SRDs. For example, if the complex is divided into nPartitions, named Par1 and Par2, Par1's compartments could be virtual partitions, while Par2's compartments are pSets.

Each compartment holds a workload. gWLM manages the workload by adjusting the compartment's resource allocation.

Short Message Service

A convenient way to send brief text messages directly to a wireless phone. There is a maximum message length of 140 characters.

Simple Network Management Protocol

One management protocol supported by HP SIM. Traditional management protocol used extensively by networking systems and most servers. Management Information Base for Network Management of TCP/IP-based internets (MIB-II) is the standard information available consistently across all vendors.

Simple Object Access Protocol

A lightweight protocol for exchange of information in a decentralized, distributed environment.

Single Sign-On

Permission granted to an authenticated user browsing to HP SIM to browse to any of the managed systems from within HP SIM without re-authenticating to the managed system. HP SIM is the initial point of authentication, and browsing to another managed system must be from within HP SIM.

single-system aware

A run type that does not support multi-system operations. Tools with this run type are only aware of the system on which they are running.

single-system aware tool

This type of tool is executed by way of SSH on the target system.

SMI CIMOM

See common information model object manager.

SMI-S provider

An industry-standard WBEM provider that implements a well defined interface for storage management. The manufacturers of host bus adapters (HBAs), switches, tape libraries, and storage arrays can integrate SMI-S providers with their systems, or provide them as separate software packages.

See also Web-Based Enterprise Management.

SNMP trap

Asynchronous event generated by an SNMP agent that the system uses to communicate a fault.

Software Distributor

The HP-UX administration tool set used to deliver and maintain HP-UX operating systems and layered software applications.

software inventory

A listing of the HP software installed on the system where the HP VCA is installed.

software update

A task to remotely update software and firmware.

spoofing

The act of a website posing as another site to gather confidential or sensitive information, alter data transactions, or present false or misleading data.

SSH client

Connects to SSH servers to perform remote task execution and file copy.

SSH server

Listens for and services requests coming in on the proper TCP/IP port, usually port 22.

status type

The classification of status messages (for example, Critical, Major, Minor, Normal, Warning, and Unknown).

Storage Management Initiative Specification

A standard management interface developed by the Storage Networking Industry Association (SNIA). SMI-S provides a common interface and facilitates the management of storage devices from multiple vendors. SMI-S uses industry-standard [common information model](#) and [Web-Based Enterprise Management](#) technology.

storage systems	SAN-attached Fibre Channel disk arrays, switches, tape libraries, or hosts (with Fibre Channel host bus adapters).
subnet	On TCP/IP networks, subnets are all systems whose IP addresses have the same prefix. For example, all systems with IP addresses that start with 10.10.10. would be part of the same subnet.
system	Systems on the network that communicate through TCP/IP. To manage a system, some type of management protocol (for example, SNMP, or WBEM) must be present on the system. Examples of systems include servers, workstations, desktops, portables, routers, switches, hubs, and gateways.
system group	A group of systems based on a system collection; a static snapshot of the source collection at the time the system group was created. Used for authorizations.
system health status	This is aggregate status all of the status sources (which can be SNMP, WBEM, and HTTP) that are supported on a target system, with the most critical status being displayed. The following are the different system health statuses that can be displayed: Critical HP SIM can no longer communicate with the system. The system was previously discovered but cannot be pinged. The system might be down, powered off, or no longer accessible on the network because of network problems. Major A major problem exists with this system. It should be addressed immediately. For systems running an Insight Management Agent, some component has failed. The system might no longer be properly functioning, and data loss can occur. Minor A minor problem exists with this system. For systems running Insight Management Agent, some component has failed but the system is still functioning. Warning The system has a potential problem or is in a state that might become a problem. Normal The system is functioning correctly. Disabled The system is disabled from monitoring but is not necessarily turned off. Unknown HP SIM cannot obtain management information about the system. Informational The system might be in a transitional or non-error state.
system identification	Identifying information about systems. This information is stored in the database. The following information is identified: - Type of management protocol on the system (SNMP, WBEM, HTTP, and SSH) - Type of HP system (server, client, switch, router, and so on) - Network name of system
System Management Homepage	An integrated piece of software used by the HP suite of HP Web-enabled System Management Software to communicate over HTTP and HTTPS. It provides a uniform set of functionality and security to HP Web-enabled System Management Software.
system properties	Properties can be set for a single system or for multiple systems at the same time and include options such as system name, system type, system sub-type, operating system version, asset number, contact information, and whether or not the system properties can be changed or updated by the discovery process.

system search	Logical grouping of systems into a collection based on information in the HP SIM database. After a search is defined, you can display the results from the system view page or associate it with a management task.
system status panel	The section of the GUI on the left of the screen that displays status information and system or event alarms.
system type	One of 12 supplied types. You can add your own based on one of these types. For example, use Server type to create MyServer type. It is still a server and is reported on in the same way, but it has your designation.
System Type Manager	A utility that enables you to modify the default behavior of the discovery and identification of objects classified as Unknown or as another category of systems are discovered and identified precisely as you require. HP SIM discovers and identifies the system and applies the new information when an Unknown system matches a rule set that you specify as the primary rule set. Furthermore, creating the new system type provides a System Link page for viewing the information returned from the system agent or from the communication protocol of SNMP .

T

target system	The system selected for a tool to run on.
task	An executed instance of an HP SIM tool, on one or more systems, with a specific set of arguments.
threshold	A preset limit that produces an event when the limit is reached or exceeded.
tool	An application, command, or script that can be executed by HP SIM on one or more systems to perform a task.
Tool definition file	The TDEF defines parameters of a tool, its execution user, toolbox, and so on in XML format.
toolbox	A defined set of tools that a user might need for a particular task, such as database administration or software management. Each HP SIM toolbox is associated with a set of tools and authorizations.
trap	An unsolicited message generated by a management agent that indicates that an event has occurred. For example, a monitored item has exceeded a set threshold or changed status. Previously called alarm. <i>See also</i> event.
type	The classification of a system, which identifies it as a standard system type. The system types are client, cluster, portable, printer, remote access device, repeater, router, server, switch, unknown, workstation, and other.

U

uncleared event status	Events that have a Critical, Major, Minor, Normal, or Informational severity and have not been cleared or deleted from the database. Events can be cleared without being deleted from the database by using the Clear events menu option. • Critical. A failure has occurred, and immediate attention is required. • Major. A failure is impending. • Minor. A warning condition exists that can escalate into a more serious problem. • Normal. These events are not a problem. • Informational. No attention required. This status is provided as useful information
unknown status	HP SIM cannot obtain management information about the system using SNMP. Although no management instrumentation information is available, the system can be pinged. It might have an invalid community string or security setting.

user	A network user with a valid login on the CMS that has been added to HP SIM.
user accounts	Accounts used to sign-in to HP SIM. These accounts associate a local Windows user account or a domain account with privilege levels and paging attributes inside HP SIM.
user group	A group of users defined on the CMS operating system that has been added to HP SIM. Members of the user group in the operating system can sign-in to HP SIM.
user rights user	A user who cannot configure the CMS. However, the user can view and run predefined reports on the CMS and all managed systems.

V

HP VCA log	A listing of all the software maintenance tasks completed by the HP VCA and reports resulting from those tasks.
version control	Referred to as the Version Control Repository Manager installed on a Windows system for Windows and Linux ProLiant systems, and Software Distributor on HP-UX operating systems. Provides an overview of the software status for all managed ProLiant or Integrity systems and can update system software and firmware on those systems programmatically using predetermined criteria. Version control identifies systems that are running out-of-date system software, indicates if an upgrade is available, and provides reasons for upgrading. For HP-UX systems, Software Distributor can be launched from an HP SIM CMS against one or more installed HP-UX systems.
Virtual Server Environment	An integrated server virtualization offering for HP-UX, Linux, and Windows servers that provides a flexible computing environment maximizing usage of server resources. VSE consists of a pool of dynamically sizeable virtual servers; each can grow and shrink based on service level objectives and business priorities. For more information, see http://hp.com/go/vse .

W

WBEM Services	HP WBEM Services for HP-UX is an HP product that uses WBEM and DMTF standards to manage HP-UX system resources.
Web-Based Enterprise Management	This industry initiative provides management of systems, networks, users, and applications across multiple vendor environments. WBEM simplifies system management, providing better access to software and hardware data that is readable by WBEM client applications.
Web-launch aware tool	A run type for tools that are launched in a web browser using a web server. WLA tools can be designed to deal with multiple systems.
Windows Management Instrumentation	An API in the Windows operating system that enables you to manage and control systems in a network.
workspace	The section of the GUI where tools appear.

X

X server	A local application that accepts X client requests and acts on them.
X Window System	A cross-platform windowing system that uses the client/server model to distribute services across a network. It enables applications or tools to run on a remote computer.
XML document	A collection of data represented in XML.

Index

A

- about, 151, 152
 - default polling tasks, 210
 - searches, 49
 - storage solutions (SNMP), 134, 137
 - version control agent, 150
- accessing
 - automatic event handling, 57
 - discovery filters, 40
- accessing the GUI, 18
- adding
 - SNMP rules, 218
- Agentless Management Service
 - AMS, 172
- agents, 23
- All c-Class Racks collection
 - discontinued, 183
- All p-Class Racks collection
 - discontinued, 183
- all scheduled tasks
 - task results list, 69
- applying
 - time filters, 58, 61
- array controllers
 - duplicate entries, 177
- attributes
 - cluster monitor, 146
- audit log, 148
- authentication
 - errors, 172
 - ESX system, 172
 - Linux system, 172
- automatic discovery, 15, 38, 40, 52, 179, 202
- automatic event handling, 15
 - accessing, 57
 - creating new task, 57
 - e-mail settings, 57
 - managing tasks, 57
 - modem settings, 57
- automatic event handling task
 - creating, 61
 - with specific event, 61

B

- banner, 20
- BC1000 blades
 - identification, 187
- biweekly data collection, 208
- blade
 - double dense, 176
- Brocade 4GbSAN Switch for HP BladeSystem, 183

C

- canceling
 - data collection, 177

- capacity
 - storage arrays, 142
- Cisco Fibre Channel switches, 179
- Cisco Gigabit Ethernet Switch Module
 - associating with enclosure, 183
- clearing
 - events, 62
- CLI
 - collections, 72
- cluster
 - identification, 213
- cluster collections, 143
 - customizing, 54
 - managing, 54
 - printing, 54
- Cluster Monitor, 179
- cluster monitor, 143
 - attributes, 146
 - CPU polling rate, 146
 - Disk polling rate, 146
 - MSCS polling rate, 146
 - polling rates, 146
 - resources, 146
 - status data fields, 143
 - system status polling rate, 146
- cluster monitor resource
 - overview, 146
 - thresholds, 145
- cluster nodes
 - management, 179
- cluster table view page, 143
 - overview, 54
- clusters, 38
 - deleting, 54
 - Hyper-V, 179
 - MSCS, 143
- CMS
 - communications, 42
 - setting locale, 190
 - system limit, 174
- collecting
 - license information, 125
- collections
 - CLI, 72
 - customizing, 72
 - discontinued, 183
 - event, 62
 - events, 72
 - saving, 62
 - storage systems, 134, 136
 - Systems Insight Manager, 72
 - tasks, 72
- command line tools
 - parameters, 82
- Command View
 - discovery, 140

- communicating
 - with systems, 35
- communication
 - errors, 173
- community strings, 52
- complex
 - deleting, 175
 - discovering, 175
 - System Page, 175
- Configure or Repair Agents, 16
 - not starting, 175
 - Windows Vista, 175
- Configure or Repair Agents task, 175
 - configuring, 175
 - fails, 175
- configuring
 - audit log, 148
 - Configure or Repair Agents task, 175
 - storage system discovery, 140
 - tool definition files, 148
- contract and warranty
 - default tasks, 210
 - status, 120, 121
 - system properties, 56
- CPU resource, 145, 146
- CPU utilization, 145
- creating
 - automatic event handling tasks, 57, 61
 - custom tools, 219
 - discovery task, 38
 - event collections, 62
 - tasks, 69
- credentials
 - deleting, 177
 - discovery, 177
 - discovery sign-in, 187
 - discovery task, 35
 - fail, 177
 - global, 35, 38
 - global sign-in, 187
 - Sign-in, 177
 - system, 35
 - system sign-in>, 187
- custom tools, 195
 - creating, 219
 - deleting, 79
 - editing, 79
 - environment variables, 80
 - managing, 79, 219
 - menu placement, 82
 - MSA, 219
 - multiple-system-aware, 219
 - running, 79
 - scheduling, 79
 - single-system-aware, 219
 - SSA, 219
 - TDEF, 219
 - web-launch tool, 219
- customizing

- cluster table view, 54
- collections, 72

D

- data collection, 208
 - append new data set, 208
 - biweekly, 208
 - canceling, 177
 - detailed analysis, 208
 - duplicate entries, 177
 - fails, 177
 - initial, 208
 - Onboard Administrator, 177
 - overwrite existing data set, 208
 - search criteria, 208
 - STDOUT error, 177
 - storage systems, 140
 - task, 177
 - upgrade issues, 177
- data collection task
 - scheduling, 208
- default tasks
 - bi weekly data collection, 210
 - daily device identification, 210
 - delete events older than 90 days, 210
 - hardware status polling for non servers, 210
 - hardware status polling for servers, 210
 - hardware status polling for systems no longer disabled, 210
 - Initial contract and warranty collection, 210
 - initial data collection, 210
 - initial hardware status polling, 210
 - Monthly contract and warranty collection , 210
 - software version status polling, 210
 - software version status polling for systems no longer disabled, 210
 - weekly check event configuration, 210
- deleting
 - clusters, 54
 - complexes, 175
 - custom tools, 79
 - discovery task, 38
 - events, 62
 - tasks, 69
- disabling
 - discovery filters, 40
 - discovery task, 38
- discovering
 - complexes, 175, 179
 - IO, 183
 - Linux servers, 182
- discovery, 16, 23
 - automatic, 38, 40, 52, 202
 - Command View, 140
 - filters, 15
 - MSCS cluster services, 179
 - storage array, 179
 - storage solutions (SNMP), 137
 - storage systems, 140

- XP P9500, 179
- discovery filters
 - accessing, 40
 - disabling, 40
 - editing, 40
- discovery tasks
 - creating, 38
 - deleting, 38
 - disabling, 38
 - editing, 38
 - enabling, 38
 - general settings, 38
 - running, 38
 - stopping, 38
- disk capacity, 145
- disk resource, 145, 146
- DL100 series systems
 - identifying, 187
- DL160 G5, 187
- DL180 G5, 187
- DMI, 202
- Dotnet, 189
- DTMF, 202

E

- e-mail paging
 - examples, 59
- e-mail settings, 57
- editing
 - custom tools, 79
 - discovery filters, 40
 - discovery task, 38
 - tasks, 69
- Emulex 1050C HBA card
 - identified as two single port HBAs, 187
- Emulex Host Bus Adapter
 - identifying, 187
- enabling
 - discovery task, 38
- enclosure
 - missing servers, 176
- enclosure view, 175
- Enhanced reports, 193
- environment variables
 - custom tools, 80
- errors
 - database initialization failed, 189
 - discovery failed, 185
 - HP Smart Update Manager connection, 185
 - HTTP status 505, 195
 - installssh.bat, 195
 - invalid credentials, 189
- ESC 3i server, 198
- ESL G3 tape library, 198
- ESX 3.x hosts, 187
- ESX 3.x servers, 187
- event collections
 - creating, 62
- event types

- dynamically added, 183
- events
 - clearing, 62, 183
 - collections, 72
 - deleting, 57, 62, 183
 - management, 57
 - rules, 57
 - server, clearing, 62
 - storage (SNMP), 134
 - storage solutions (SNMP), 138
- events task
 - running, 62
 - scheduling, 62
- examples, 23
 - clearing server events, 62
 - command line tool parameters, 82
 - e-mail paging, 59
 - system properties, 56
 - web launch tool parameters, 82
- execute-as user, 23

F

- failover, 179
- fault management, 15
- Firefox, 18, 194

G

- global credentials, 38
- global protocol settings, 38, 202
 - setting, 208
 - storage systems, 140
- globalsettings.props
 - SnmpTrapPortAddress, 202
- graphical user interface see GUI
- GUI
 - banner, 20
 - features, 18
 - Home page, 20
 - requirements, 18
 - signing in, 18

H

- hardware status polling for non servers, 213
- hardware status polling for servers, 213
- Hardware Status Polling task
 - no longer works, 195
- health monitoring, 15
- health status, 210, 213
 - MSA G3, 183
 - types, 52
- Home page, 20
- host names
 - long, 183
 - truncated, 183
- hosts file, 182
- hosts files
 - extensions, 214
 - managing, 38
- HP Insight Control performance management, 125

- HP Insight Control power management
 - 24-hour graph, 183
 - incompatible server, 183
 - license, 183
 - temperature graph, 183
- HP Insight Control virtual machine management, 179
- HP Insight Dynamics, 179
- HP Insight Remote Support, 189
- HP Insight Remote Support Pack
 - contract and warranty status, 120, 121
 - default tasks, 210
 - system properties, 56
- HP Logical Server, 179
- HP Network-attached Storage systems
 - discovering, 187
- HP ProLiant SNMP Agent, 183
- HP ProLiant WBEM Providers, 193
- HP Service Pack for ProLiant, 187
- HP Serviceguard package, 179
- HP SIM
 - installation errors, 189
 - upgrading, 196
- HP Smart Update Manager, 185
- HP SMH, 177
- HP Version Control, 150, 151, 152
- HP-UX, 208
 - empty, 177
 - managed systems, 23
- HTTP, 202

I

- identification, 187
 - cluster, 213
 - management processor, 213
 - SNMP, 218
 - storage solutions (SNMP), 137
- identifying
 - BC1000 blades, 187
 - complex, 187
 - DL100 series systems, 187
 - Emulex 1050C HBA card, 187
 - Emulex Host Bus Adapter, 187
 - management processors, 187
 - xw25p Blade Workstation, 183
- Ignite servers, 190
- iLO, 52, 179, 182
 - associations, 182
 - firmware version, 183
- iLO associations
 - not displaying, 182
- iLO2, 183
- incorrect drive information, 183
- indications, 15
- initial data collection, 208
- Initial ProLiant Support Pack Install task, 195
- Insight Control virtual machine management, 185
- Insight Dynamics - USE, 179
- Insight Management Advisor, 183
- Insight Manager 7, 208

- Install OpenSSH task, 195
- Install Software and Firmware task, 195
- installation
 - Oracle database, 189
 - typical, 189
- installing
 - HP SIM errors, 189
 - MSDE errors, 189
- Integrated Lights-Out see iLO
- integration, 151
- Internet Explorer, 18, 189
 - maximum URL length, 190
 - response time, 173
- IP address, 70
- IPX address, 70

J

- Java 1.5, 177
- Java Virtual Machine, 183
- JRE, 187

K

- Kernal Configuration (kcweb), 195

L

- legend, 20
- license management, 125
- license manager, 190
 - subscription expiration, 190
- licensing
 - assigning licenses, 125
 - collecting license information, 125
 - iLO, 125
 - managing licenses, 125
 - ProLiant Essentials, 125
- Linux, 208
 - HP VCA, 150
- Linux ProLiant agents
 - installing, 182
- Linux servers
 - discovering, 182
- log.properties, 148

M

- Managed Environment, 47
- managed environment, 190
- managed systems
 - communications, 42
 - HP-UX, 23
 - overview, 23
 - performance, 191
 - setting up, 23
 - Windows, 23
- management, 152
- management agents, 23
- management processor, 183
 - identification, 213
- management processors
 - identifying, 187

- PA-RISC, 182
- management protocols, 23
- managing
 - automatic event handling tasks, 57
 - cluster collections, 54
 - CMS communications, 42
 - custom tools, 79, 219
 - discovery task, 38
 - events, 57
 - hosts files, 38
 - licenses, 125
 - SSH keys, 16
- Matrix infrastructure orchestration
 - discovering, 183
- McDATA 4Gb SAN Switch for HP BladeSystem
 - associating with enclosure, 183
- MIB, 218
 - internet management, 202
 - rules, 218
 - vendor, 202
- mib, 191
- Microsoft Windows 2008 MSCS cluster, 179
- ML370 G5 server, 183
- modem settings, 57
- monitoring
 - health, 15
- Mozilla, 190, 195
 - response time, 173
- MSA
 - custom tools, 219
- MSA G3
 - health status, 183
- MSCS
 - clusters, 143
- MSCS cluster services
 - discovery, 179
- MSCS resource, 146
- MSDE, 196
 - installing, 189
- multiple-system-aware
 - custom tools, 219
- mxagentconfig, 172, 175, 195
- mxauthenticationexception, 195
- mxinventory processes, 177
- mxnodesecurity, 35, 195
- mxstm, 218

N

- name mismatches, 179
- naming restrictions, 179
- National Language Support, 189
- navigating
 - Home page, 20
- nPars, 175

O

- Onboard Administrator, 179, 191
 - data collection, 177
- OpenSSH, 191, 196

- typical install, 189
- operating system
 - inconsistent version, 187
- Oracle, 189
- orphans
 - preventing, 179
- overview, 125
 - managed systems, 23
 - reporting, 64
 - storage solutions (SNMP), 134
 - storage systems, 134, 136

P

- parameters
 - examples, 82
- Pegasus WMI Mapper, 177
- performance
 - managed systems, 191
- performance management, 174
- Peripheral Device (pdweb), 195
- ping, 70, 192
- polling tasks
 - customizing, 213
 - default, 210
- port 162, 202
- printing
 - cluster collections, 54
- privilege elevation
 - login issues, 193
- ProLiant iLO Advanced
 - licensing, 190
- ProLiant Support Pack, 23
- ProLiant xw2x220c Blade Workstation, 176
- Property pages, 193
- protocol settings
 - global, 183
- protocols, 23, 205
 - DMI, 202
 - global, 202
 - HTTP, 202
 - setting, 202
 - setting global, 140
 - single system, 202
 - SNMP, 202, 208, 213
 - WBEM, 35, 202, 208
 - WMI Mapper Proxy, 37

Q

- quiesce, 119

R

- related documents, 235, 236
- Remote Registry service, 175
- Replicate Agent Settings task, 195
- reporting, 15
 - graph labels, 193
 - overview, 64
 - snapshot comparison, 193
 - snapshot comparisons, 16

- storage array capacity, 142
- storage systems, 141
- views, 64
- reports, 64
 - data collection, 16
 - inventory, 16
 - storage systems, 141
- requirements
 - GUI, 18
- resources
 - cluster monitor, 145, 146
 - thresholds, 145
- response time, 173
- ROM BIOS, 196
- RPM Package Manager tools
 - no longer work, 195
- rules
 - SNMP, 218
 - System Type Manager, 218
- running
 - custom tools, 79
 - discovery task, 38
 - events task, 62

S

- saving
 - collections, 62
- scheduling
 - clear events task, 62
 - custom tools, 79
 - event tasks, 62
 - tasks, 69
- search, 20
- search criteria, 208
- searching
 - advanced, 49
 - basic, 49
 - hierarchical displays, 49
- security, 16, 193
 - role-based, 15
- security alerts, 18
- server
 - protocols, 205
- server connections
 - increase size, 173
- setting up
 - managed systems, 23
 - managed systems - HP-UX, 23
 - managed systems - Linux, 23
 - managed systems - Windows, 23
- settings
 - browser, 18
- sign-in, 194
- signing in
 - GUI, 18
- Simple File Sharing, 187, 189
- Single Sign-On, 179
- single system protocol settings, 202
 - setting, 208

- single-system-aware
 - custom tools, 219
- SMBIOS, 196
- SMI-S, 179
- SMI-S providers
 - storage systems, 140
- SNMP, 23, 202, 208, 213
 - adding rules, 218
 - port 162, 202
 - SnmpTrapPortAddress, 202
 - trap, 57
 - traps, 213
- SNMP Agents, 179
- SNMP agents, 197
- SNMP settings, 194
- SNMP traps, 194
- software
 - status, 53
- Software/Firmware, 194
- Software/Firmware Baselines
 - junk values, 152
- SQL Express 2005 SP2, 196
- SQL Server
 - ports, 189
- SSA
 - custom tools, 219
- SSH, 23
 - domain support, 194
- SSH key, 175
- SSH keys
 - managing, 16
- SSL, 16
- status
 - software, 53
 - system, 52
 - WBEM status, 54
- status polling
 - hardware status polling, 213
 - software status polling, 213
- STDERR error, 175
- STDOUT error
 - data collection, 177
- stopping
 - discovery task, 38
 - tasks, 69
- storage array
 - discovery, 179
- storage host
 - data collection fails, 177
- storage solutions (SNMP)
 - about, 134
 - configuring event collection, 138
 - discovery, 137, 140
 - overview, 134, 138
 - searching for, 138
- storage systems (SMI-S)
 - discovery, 140
 - overview, 134, 136
 - SMI-S providers, 140

- storage systems, 141
- viewing, 134
- viewing array capacity, 142
- WBEM event indications, 140
- subscribing
 - WBEM indication events, 140
- support, 235
- system
 - status, 52
 - WBEM status, 54
- system collections
 - customizing, 51
 - managing, 51
 - printing, 51
- system key, 20
- system monitoring
 - resume, 55
 - suspend, 55
- system page, 138, 202, 208
 - protocols, 205
- system properties
 - examples, 56
 - set for multiple systems, 56
- system resource, 146
- system status, 194
- system status panel, 20
- system tab
 - protocols, 205
- system table view page, 49, 70, 138, 208
 - overview, 51
- System Type Manager
 - SNMP rules, 218
- systems
 - deleting, 51
- Systems Insight Manager
 - collections, 72

T

- target selection
 - troubleshooting, 194
- task instance, 69
- task results
 - viewing, 62, 70
- tasks, 15
 - collections, 72
 - command line, 195
 - creating, 69
 - Daily Identification, 177
 - data collection, 208
 - default, 210
 - deleting, 69
 - editing, 69
 - instance, 69
 - invalid characters, 195
 - paging, 58
 - polling, 210
 - scheduling, 69
 - stopping, 69
 - track status, 69

- user privileges, 69
- TDEF see tool definition files
 - custom tools, 219
- temperature sensors, 198
- thresholds
 - cluster monitor, 145
- time filters
 - applying, 58, 61
- tool definition files, 148
- tools, 16, 195
 - authorization, 195
 - customized, 15
 - Kernal Configuration (kcweb), 195
 - launching, 195
 - Peripheral Device (pdweb), 195
 - ping, 70
- Trust Platform Module, 182
- trust relationships, 195

U

- unsupported characters
 - database user names and passwords, 189
 - operating system, 189
- upgrading
 - data collection, 187
 - HP SIM, 196
 - identification, 187
 - Oracle JDBC driver, 196
 - running Daily Device Identification task, 187
- UUID, 196

V

- v0 keys, 190
- VCEM
 - menus, 196
- viewing
 - task results, 62, 70
- virtual machine hosts, 179
- virtual machines, 197
- VMware
 - subscriptions, 198
- VMWare ESX
 - property pages, 193
- VMware ESX Server, 187

W

- WBEM, 23, 187, 202, 208
 - events, 198
 - status, 54
- WBEM connections, 177
- WBEM events
 - subscribing, 182, 183
- WBEM indications, 198
- web browsers
 - communication errors, 173
 - requirements, 18
- web launch tools
 - parameters, 82
- web-launch tool

- custom tools, [219](#)
- Windows
 - managed systems, [23](#)
- Windows 2000, [195](#)
- Windows 2008, [175](#)
- Windows 2008 64-bit, [196](#)
- Windows Vista
 - Configure or Repair Agents, [175](#)
 - User Account Control features, [196](#)
- Windows XP, [196](#)
- Windows XP SP2, [175](#)
- Windows XP SP3, [191](#)
- WMI Mapper
 - service, [198](#)
- WMI Mapper Indications
 - service, [198](#)
- WMI Mapper proxy, [198](#)

X

- XP P500
 - WBEM indications, [198](#)
- xw25p Blade Workstation
 - identifying, [183](#)